

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 11, Number 11

November 2011

UNITED KINGDOM

Extension Of Compulsory Audits To Additional Sectors Sought By ICO

*By Rohan Massey, of McDermott Will & Emery UK LLP,
London.*

Speaking at the 10th annual data protection compliance conference in London held October 12-13, 2011, UK Information Commissioner Christopher Graham said that compulsory audits should be extended to local government, the health service and the private sector in order to ensure compliance with the law.

Currently the only compulsory data protection audit powers the Information Commissioner's Office (ICO) has are for central government departments. For all other organisations, the ICO has to win consent before an audit can take place.

Businesses remain the sector generating the most data protection complaints. Despite this, just 19 percent of companies contacted by the ICO accepted the offer of undergoing an audit. The ICO has written to 29 banks and building societies, and so far only six (20 percent) have agreed to undergo an audit. The insurance sector has also shown reluctance in this area. Of the 19 companies contacted this year by the ICO, only two agreed to an audit.

Christopher Graham said: "Something is clearly wrong when the regulator has to ask permission from the organisations causing us concern before we can audit their data protection practices. Helping the healthcare sector, local government and businesses to handle per-

sonal data better are top priorities, and yet we are powerless to get in there and find out what is really going on".

He insisted that extended audit powers are urgently needed, and has confirmed that the ICO is preparing a business case for the extension of its Assessment Notice powers under the Coroners and Justice Act 2009 "to these problematic sectors".

'Badge of Honour'?

Mr. Graham has told businesses that they should see consensual audits as a "badge of honour", but the message appears to have fallen on deaf ears. The reality appears to be that businesses are not confident that a badge of dishonour won't quickly follow, and even a fine, should they expose themselves to an internal examination by the ICO.

But, as is frequently pointed out, by ignoring the ICO's requests for voluntary audits, businesses face higher fines if something does go wrong. The ICO has previously made clear that failure to report security breaches would result in tougher sanctions in the event that a data breach were to occur. Refusing to be audited and then failing to report a serious breach could result in a substantial fine.

Some businesses may believe that they exist under the ICO's radar. For more high profile companies, however, the perceived risks of exposing their businesses to the ICO's scrutiny appear to outweigh the benefits.

At the moment they have a choice, but if Mr. Graham has his way, that will change.

Rohan Massey is a Partner in the IMPT Group, McDermott Will & Emery UK LLP, London. He may be contacted at rmassey@mwe.com.