



**Information Commissioner's Office**  
Promoting public access to official information  
and protecting your personal information

## **Press Release**

**Strictly embargoed until 00.01 on 29 October 2008**

### **Privacy watchdog calls on CEOs to take responsibility for data protection safeguards**

The number of data breaches reported to the Information Commissioner's Office (ICO) has soared to 277 since HMRC lost 25 million child benefit records nearly a year ago. New figures, released today by the ICO, include 80 reported breaches by the private sector, 75 within the NHS and other health bodies, 28 reported by central government, 26 by local authorities and 47 by the rest of the public sector. The ICO is investigating 30 of the most serious cases.

In a [speech](#) today Richard Thomas, the Information Commissioner, will highlight the risks associated with large databases, the need for tougher sanctions to deter data breaches and he will call on chief executives to take responsibility for the personal information their organisations hold. Arguing that information can be a toxic liability, he will challenge CEOs to ensure that the amount of data held is minimised and that robust governance arrangements are in place. Richard Thomas will argue that accountability rests at the top. CEOs must make sure that their organisations have the right policies and procedures in place, that privacy by design features are incorporated in the technology their organisations use and that staff are properly trained to counter the risks.

The Information Commissioner will say: 'It is alarming that despite high profile data losses, the threat of enforcement action, a plethora of reports on data handling and clear ICO guidance, the flow of data breaches and sloppy information handling continues. We have already seen examples where data loss or abuse has led to fake credit card transactions, witnesses at risk of physical harm or intimidation, offenders at risk from vigilantes, fake applications for tax credits, falsified Land Registry records and mortgage fraud. Addresses of service personnel, police and prison

officers and battered women have also been exposed. Sometimes lives may be at risk.

Richard Thomas continues: 'The number of breaches brought to our attention is serious and worrying. I recognise that some breaches are being discovered because of improved checks and audits as a welcome result of taking data security more seriously. More laptops have now been encrypted and thousands of staff have been trained. But the number of breaches notified to us must still be well short of the total. How many PCs and laptops are junked with live data? How many staff do not tell their managers when they have lost a memory stick, laptop or disc? Many losses are probably simply undetected.'

Richard Thomas continues: 'Personal information is now the lifeblood of government and business. Used properly and intelligently, personal information can lead to better customer service, improved efficiency, more effective law enforcement and protection of the vulnerable and a better quality of life for everyone. But this means respecting and protecting people's privacy and personal information - data protection - has never been more important. As government, public, private and third sectors harness new technology to collect vast amounts of personal information, the risks of information being abused increases. It is time for the penny to drop. The more databases that are set up and the more information exchanged from one place to another, the greater the risk of things going wrong. The more you centralise data collection, the greater the risk of multiple records going missing or wrong decisions about real people being made. The more you lose the trust and confidence of customers and the public, the more your prosperity and standing will suffer. Put simply, holding huge collections of personal data brings significant risks.'

The ICO has long argued that its powers, sanctions and resources - fixed in another era - are now wholly inadequate and that a stronger approach is required to help prevent unacceptable information handling. Earlier this year Parliament decided that the ICO should have the power to impose substantial penalties for deliberate or reckless breaches. The ICO is working with the government to ensure this measure is implemented as soon as possible. The threat and reality of substantial penalties will concentrate minds and act as a real deterrent. The data protection notification

fee for the largest organisations needs to be increased to give the ICO the resources we need to do its job properly. The ICO is also looking forward to new powers to undertake inspections and audits of data controllers.

Richard Thomas is sceptical about placing a statutory duty on organisations to notify people directly whenever a breach occurs; it is doubtful that an appropriate law could satisfactorily distinguish in advance between situations where notification is needed and those where it is not. Each breach carries different levels of risk and, consequently, requires a different response.

Following serious data breaches in the past year, the Information Commissioner's Office has taken enforcement action against Orange Personal Communications Services Ltd, HMRC, the Ministry of Defence, the Department of Health, Virgin Media Ltd, Skipton Financial Services, the Foreign and Commonwealth Office, Carphone Warehouse and Talk Talk.

## **ENDS**

If you need more information, please contact the ICO press office on 020 7025 7580 or visit the website at: [www.ico.gov.uk](http://www.ico.gov.uk)

### **Notes to Editors**

1. A plethora of reports have been issued: A Surveillance Society, Home Affairs Select Committee; HMRC breach, Kieran Poynter (PWC) and IPCC; Ministry of Defence breach, Edmund Burton; Data Handling in Government, Sir Gus O'Donnell, Cabinet Secretary; Data sharing, Thomas/Walport; Criminality information, Sir Ian Magee
2. The following sources of advice are available: ICO guidance and advice from staff; ICO Privacy Impact Assessments Handbook; Managing Information Risk, HMG; Directors' Guides to Managing Information Risk, IAAC, ISAF, BT; Data Handling in Government
3. Organisations that experience a data breach are encouraged to report it to the ICO immediately
4. A table of the breaches is available from the ICO press office
5. The Criminal Justice and Immigration Act 2008 provides the ICO with the power to impose substantial civil penalties for deliberate or reckless breaches of data protection principles which are serious and could cause substantial damage or distress
6. The Information Commissioner's Office promotes public access to official information and protects personal information. The ICO is an independent body with specific responsibilities

set out in the Data Protection Act 1998, the Freedom of Information Act 2000, Environmental Information Regulations 2004 and Privacy and Electronic Communications Regulations 2003.

7. For more information about the Information Commissioner's Office subscribe to our e-newsletter at [www.ico.gov.uk](http://www.ico.gov.uk)
  
8. Anyone who processes personal information must comply with eight principles, which make sure that personal information is:
  - Fairly and lawfully processed
  - Processed for limited purposes
  - Adequate, relevant and not excessive
  - Accurate and up to date
  - Not kept for longer than is necessary
  - Processed in line with your rights
  - Secure
  - Not transferred to other countries without adequate protection