First published in the Law Society Gazette (December 2007)

The Child Benefit Data Fiasco

By Ibrahim Hasan

On Saturday morning my better half received a letter from the acting chairman of HM Revenue and Customs (HMRC) personally apologising for the loss of our family's Child Benefit data. In the past few days 7.25 million such letters have been sent out. Little wonder that the post seems slower than usual.

This unprecedented apology comes as a result of recent events which culminated in the resignation of the then chair of HMRC and an emergency statement to Parliament by Alistair Darling. The Chancellor was forced to admit that his department had managed to lose 25 million Child Benefit records. The lost (or stolen) information included the names, addresses, dates of birth, National Insurance numbers and, where relevant, bank details of claimants.

According to the BBC, two password-protected discs containing the data were sent by HMRC in Newcastle to the National Audi Office in October. The package was sent by courier and it appears that it did not arrive at its destination. A further package was sent by recorded post which did arrive. The Police have been called in but, at the time of writing, nothing has been found.

The Government doesn't seem to be having much luck complying with its data protection obligations at the moment. On 13th November, the Information Commissioner Office (ICO) announced that he had found the Foreign and Commonwealth Office (FCO) in breach of the Data Protection Act 1998 (DPA) following an investigation into a security breach at the online application facility for UK visas. The breach meant that the personal data of people applying for visas to enter the UK was visible to others visiting the website. The ICO has now obtained a formal undertaking from the FCO agreeing to comply with the principles of the DPA. Failure to do so will result in further enforcement action. More DPA failures were alleged in this week's News of the World. Apparently an ex-contractor at the Department for Work and Pensions (DWP) had two discs with thousands of benefit claimants' details for more than a year. The woman told the News of the World she forgot to return them after she stopped working for the DWP a year ago. The unencrypted discs revealed the type of benefits paid, but a DWP spokesman said they did not contain bank details.

Lack of understanding and implementation of the DPA is at the heart of all these failings. The Act is designed to protect the privacy of individuals through regulating the processing of their personal data. At its heart are the eight Data Protection Principles which govern everything from collection through to archiving and destruction of personal data. Breach of one of the principles is not in itself a criminal offence but it can lead to an investigation and enforcement action by the Information Commissioner.

Principle 7 states:

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

Note the use of the words "technical" and "organisational" The Child Benefit fiasco suggests that HMRC needs to have a root and branch review of security policies and procedures. Searching questions need to be asked. For example, why was such sensitive data not encrypted but merely password protected? I once read somewhere that the most common password in this country is "password". Hopefully, if criminals do have the CD's, they don't read the Gazette!

The Chancellor blamed mistakes by "junior officials" at HMRC, whom he said had ignored security procedures .The question arises, why was a junior member of staff able to access such sensitive data and why was he able to save such a large amount of data on a CD? Principle 7 also places an obligation on the data controller to take reasonable steps to ensure the reliability of any employees who have access to personal data. This is widely interpreted to mean that employees should be made aware of the sensitivity of the data they handle, access to it should be on a strict need to know basis and they should be made aware of their, as well as the organisation's, legal responsibilities.

There is certainly a lot of blame being laid at the door of HMRC at the moment. But is their a claim? Can 7.5 million people sue HMRC or even the Government? Section 13 of the Act states that an individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the Act is entitled to compensation for that damage. However the difficulty of any litigants will lay in proving causation. Many experts have predicted that fraudsters who may have possession of the data will sit on it for months if not years before making use of it. Unfortunately the Act does not allow a claim for distress alone.

The fallout from all the recent data loss stories has finally meant that a government which seemed to be treating the DPA (and sometimes the Information Commissioner) as a barrier to its own policy agenda (e.g. ID cards, e government and more multi agency information sharing) has been forced to give both the respect they deserve. During the first Prime Minister's Questions after the Child Benefit story broke, Gordon Brown announced that the ICO is to be given the power to make "spot checks" on organisations holding personal data.

The Act does not currently require a data controller to notify either the ICO or the data subjects that their data has been lost or stolen. Pressure is now mounting on the government to introduce such a law. In September, a House of Lords committee repeated calls for a data-breach notification law following a report that detailed the findings of an enquiry into internet security.

Criminal charges for data security breaches could be brought against both organisations and individuals if the Information Commissioner gets his way. He has repeated his calls for people who are grossly negligent with individuals' personal data to face such action.

With spot checks on the horizon, now is a good time for organisations holding personal data, including solicitors, to revisit their data protection and data security policies. Thought must also be given to raising awareness amongst staff and service providers and reviewing contractual provisions. Having advised on major public sector projects, I know from first hand experience that the data protection provisions are often the last and least discussed clauses in the contract. From now on I suspect that they will receive the attention that they rightly deserve. Data Protection will never be cool or sexy but recent events have shown that a disregard for it can have serious consequences for both the organisations and individuals involved.

Ibrahim Hasan is a director of Act Now Training and a consultant with IBA Solicitors. He produces the UK's first Freedom of Information podcast. See www.informationlaw.org.uk

---