Legal Update

Data protection: More powers for the information commissioner

Ewan Nettleton

is a senior associate solicitor in the Intellectual Property Department at Bristows. He specialises in Intellectual Property Law with an emphasis on litigation. He has an MA in Chemistry and a DPhil in Protein Chemistry and is particularly interested in matters relating to the IT and pharmaceutical industries.

Charles Willison

is a trainee solicitor at Bristows. He is currently sitting in the Corporate Department. He has a BA in Economics.

ABSTRACT The Coroners and Justice Act 2009, the Data Protection (Monetary Penalties) (Maximum Penalties and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010 came into full force on 6 April 2010, increasing powers available to the United Kingdom's data protection watchdog, the Information Commissioner's Office (ICO). The additions include the power to request compulsory audits of certain 'data controllers' (organisations, such as database marketers, which are responsible for processing personal data) and the power to issue monetary fines of up to £500,000 for serious data protection breaches. These changes represent a significant strengthening of the ICO's powers. However, the compulsory auditing powers are limited and, at least for now, apply only to the public sector. The extent to which these powers can be effective, their possible ramifications for database marketers and other data controllers and further changes that may be made further down the line are evaluated below.

Journal of Database Marketing & Customer Strategy Management (2010) 17, 132–137.

doi:10.1057/dbm.2010.5

Keywords: information commissioner's office; data protection; assessment notice; monetary penalty

BACKGROUND

Issues of data protection have been very much in the public eye in recent years with report after report of high-profile losses of personal data held by large public and private sector organisations. With advances in modern technology, huge amounts of data can be carried around on a laptop or memory stick, and sensitive data have been lost when such items have gone astray.

Various legislative changes have been made to combat this, including adding to the

powers at the disposal of the UK Information Commissioner's Office (ICO) as we have explained previously.¹ However, while progress is being made, it seems that some underlying problems remain. In a press release as recent as 11 November 2009,² the ICO stated that *the majority of organisations get data protection right, but regrettably a significant minority of management teams are failing to take data protection seriously enough. Unacceptable amounts of data are being stolen, lost in transit or mislaid by staff.*

Correspondence:
Ewan Nettleton
Bristows, 100 Victoria
Embankment, London,
EC4Y 0DH, UK
E-mail: ewan.nettleton@
bristows.com

This press release followed a string of data protection losses coming to light, including the loss of the personal data of 51 000 customers contained on a backup tape by the insurer Zurich, reported just the month before.³ Using the powers it had available at the time, the ICO found Zurich to be in breach of the Data Protection Act 1998 (DPA) and issued an enforcement notice, which led to Zurich signing undertakings to ensure that appropriate data protection safeguards are in place in future.⁴

Since that time, recent changes to the legislation mean the ICO has additional powers at its disposal. The remainder of this article concentrates on two of these – the power to serve assessment notices and the power to issue monetary penalties – though it should be noted that these are just two of many recent developments in the area of data protection enforcement.

RECENT LEGISLATIVE CHANGES

It is perhaps no coincidence that, on the day after the 11 November press release, the Coroners and Justice Act 2009 received royal assent, ushering in greater powers for the ICO, with a range of amendments to the DPA. Perhaps the most significant of these was a mechanism for the ICO to conduct compulsory audits of certain data controllers, using the so-called *assessment notices*. Data controllers receiving such notices will have to allow the Commissioner to audit their arrangements by, for example, entering their premises to inspect or examine documents and other materials, and to inspect how personal data are processed on the premises.

The ICO's power to serve assessment notices

The mechanism by which the assessment notice procedure operates is partly prescribed by the DPA and partly by a code of practice from the ICO. At the

time of writing, the latter is due to come into force in April 2010.

New section 41A(1) of the DPA gives the Commissioner the power to serve an assessment notice on a data controller to determine *whether the data controller has complied or is complying with the data protection principles*. This is a form of compulsory audit, as opposed to the existing ICO framework of consensual audits, which represents a significant change. However, under section s.41C(1) of the DPA, the Commissioner must prepare and follow a code of practice setting out the way in which his powers concerning assessment notices are to be exercised. In particular, the code must specify the factors to be considered when the Commissioner decides whether to serve an assessment notice, describe those documents and information that are and are not to be inspected, and deal with the nature of interviews, inspections and examinations under the notices and with the preparation, issuing and publication of assessment reports.

The ICO announced a draft code of practice⁵ and sought input from the public by way of a consultation on 12 February 2010⁶ in anticipation of publishing a final code of practice in April 2010. The consultation on the draft code closed on 24 March 2010 and the results are expected shortly. Importantly, the consultation proposed the following procedures for the implementation of assessment notices. Under the proposed code, assessment notices will only be served when

- a risk assessment has been conducted, indicating a high probability that personal data are not being processed in compliance with the DPA, and there is a significant likelihood of damage and distress to individuals; and,
- the data controller has failed to respond to a written request from the Commissioner to undertake an audit or has refused consent to such an audit, without adequate reasons.

The risk assessment will involve considering and weighing-up a range of factors including: the compliance history of the data controller, communications with the controller that demonstrate a lack of compliance, business intelligence (such as news reports), audits and statements of control that demonstrate compliance problems, the volume and nature of the personal data being processed, and the perceived impact on individuals of any potential non-compliance. The ICO intends to continue its practice of requesting a consensual audit in the first instance, but will then consider whether to serve an assessment notice for a compulsory audit if permission is refused and the Commissioner perceives there to be sufficient risk.

The draft code as published suggests that the scope for the ICO to serve assessment notices will be very broad, and it adds a significant new power to the ICO's armoury. For the first time, subject to the limitations discussed below, it gives the ICO a compulsory means to audit data controllers, and should allow the Commissioner to keep a check on those who do not agree to a voluntary audit to ensure compliance with the DPA.

Limitations of the assessment notice framework

That said, there are some significant limitations of assessment notices. The primary limitation is that these notices may, as things stand, only be served on public bodies. Specifically, section s.41A(2) states that assessment notices may only be served on: (a) a government department, (b) a public authority or (c) a person designated by the Secretary of State. However, in its 11 November 2009 press release,² the ICO noted that in the previous 2 years, over 200 of the 711 organisations reporting security breaches were from the private sector. Furthermore, the ICO has explicitly requested several times that the scope of assessment notices be broadened to

encompass the private sector, with statements made to this effect at three readings of the Coroners and Justice Bill⁷⁻⁹ and in the press release that accompanied the draft code of practice consultation published on 12 February 2009. The ICO has also said that the code of practice has been drafted so as to provide advice on the ICO's auditing framework to both public and private sector organisations, and thus it is also relevant to data controllers such as database marketers in the private sector (if, for example, they receive a request from the ICO for a consensual audit). The ICO suggests that organisations use the code as a checklist to evaluate and improve their current procedures, and/or to make sure that new online services are delivered in a privacy-friendly way.

Although section 41A(2)(c) allows additional persons to be designated as subject to the new compulsory auditing procedures, this would require approval of the Secretary of State and a consultation of the persons who represent the interests of the new groups to be covered.

Practically speaking, it seems unlikely that this will be the mechanism used to extend assessment notices to the private sector. Nonetheless, the ICO's statements make explicitly clear its wish *to undertake compulsory audits in the rest of the public and private sectors*.¹⁰

The ICO's responses to the readings of the Coroners and Justice Bill also highlighted further limitations of the amendments to the DPA. First, the ICO requested a sanction against organisations that fail to comply with the assessment notice requirements. It suggested that such failures should constitute either a criminal offence modelled on section 47 of the DPA (which deals with the failure to comply with an information or enforcement notice) or contempt of court. As the ICO has put it, without such a form of sanction, there is no pressure to comply and no consequence for a failure to do so.

Perhaps surprisingly, another notable fettering of the *bite* of the assessment notice came from the ICO itself. The ICO seems to have decided not to issue monetary fines for breaches of data protection principles that come to light by way of assessment notices. This policy is set out in the statutory guidance issued by the ICO on monetary fines discussed further in the next section.¹¹ That said, the ICO does not give any absolute assurance that no enforcement action will be taken following an audit, and one would expect further consequences to follow if a major breach is identified and the data controller fails to remedy the situation within an appropriate time.

The ICO's power to issue monetary penalties

Another important additional power that is now at the ICO's disposal is the ability to issue monetary penalties. In contrast to the assessment notices, these penalties can apply to data controllers in both the public and private sectors. The Data Protection (Monetary Penalties) (Maximum Penalties and Notices) Regulations 2010 and the Data Protection (Monetary Penalties) Order 2010 allow the ICO to impose financial penalties of up to £500 000 for serious breaches of the DPA. Both came into force on 6 April 2010, and the ICO published guidance on when and at what level these fines will be issued on 12 January 2010. This guidance was laid before the Houses of Parliament as required by section 55C DPA.

The guidance suggests there will be three main issues to be considered when the ICO decides whether a monetary penalty should be imposed. The first involves assessing whether there has been a *serious contravention* of the data protection principles. The Commissioner will seek to assess this in light of the reasonable expectations of individuals in society, and notes in the guidance that *it is possible*

that a single breach of a data protection principle may be sufficient to meet this threshold. The fact that a single breach can warrant a fine suggests that this aspect could be fulfilled in situations like many of the high-profile breaches that have hit the press in recent years.

Second, the ICO must determine whether there has been a *contravention of a kind likely to cause substantial damage or distress*. The effects of a contravention considered will extend to distress as well as financial damage, and this aspect is to be assessed with regard to the data's importance, value, degree, amount or extent. This suggests that it too will have a broad threshold.

Finally, either (a) the breach of the data protection principles must be deliberate or (b) the data controller must have known there was a risk that such a breach could occur and have taken no reasonable steps to prevent it. Whether the breach is deliberate will turn on the facts of the particular breach, whereas the second possibility will be assessed objectively against the standard of a reasonably prudent data controller. According to the guidance, adequate steps to prevent a breach may include: risk assessments being employed by the controller, adequate procedures and policies having been in place for the handling of personal data, and indications of good governance and auditing arrangements.

Will the monetary fines have the desired effect?

The ability to issue monetary fines represents a significant increase in the powers of the ICO. The broad basis with which a fine can be issued, suggested by the accompanying guidance, leaves little doubt that further data protection breaches of the kind reported previously are likely to lead to large monetary fines from the ICO in the future. However, the fundamental role of the ICO is to seek to ensure

compliance with the DPA from the outset, and the value of such monetary fines may lie in their deterrent effect, raising the question of whether they will encourage the *significant minority* of data controllers referred to in the ICO's 11 November press release to operate data protection procedures that are compliant with the DPA. Although the fines could be large, they are still significantly smaller than the financial penalties meted out by other sector-specific watchdogs such as the FSA, which, for example, fined three HSBC insurance firms in excess of £3 000 000 for loss of customers' personal data in July 2009.¹²

CONCLUSIONS

The huge quantities of personal data held by large organisations in the public and private sectors, coupled with the deep public concern for protection of personal data stoked by high-profile data losses, have led to various new powers being given to the United Kingdom's data protection watchdog, the ICO. In particular, and for the first time, the ICO can carry out compulsory audits to identify data protection breaches by issuing assessment notices in appropriate circumstances. As things stand, these audits are limited to the public sector, and the lack of consequences may mean that the assessment notices lack *bite*. However, the ICO will continue to request consensual audits of private sector organisations, and it has made crystal clear its desire to extend the compulsory audits to the private sector in the future, and worries over bad publicity alone may make these an effective tool when they are applied. In addition, monetary fines can now be imposed on private and public sector organisations for serious data protection breaches, and this too represents a significant expansion of the ICO's armoury. However, while the penalties will provide a further reason for responsible data controllers to adhere to the rules, their

relatively low level compared with those levied by the likes of the FSA may not be enough to discourage the hard core who the ICO suggests continue to flout the rules.

REFERENCES AND NOTES

- 1 See article entitled *Data protection: Tougher enforcement and increased power for the information commissioner?* published in this journal, Vol. 15, No. 3, pp. 207–212. As this article explains, the data protection rules coupled with rules relating to unsolicited marketing communications set out in the United Kingdom's Privacy and Electronic Communications Regulations are the principal rules with which the ICO expects database marketers to comply.
- 2 ICO press release entitled *Burglary and theft account for a third of data security breaches* dated 11 November 2009 (see http://www.ico.gov.uk/upload/documents/pressreleases/2009/nadpo_111109.pdf).
- 3 BBC News article entitled *Personal data of 51,000 lost* dated 22 October 2009 (see <http://news.bbc.co.uk/1/hi/business/8320290.stm>). It should be noted that the ICO press release cited in the next footnote refers to loss of data of 46 000 of Zurich's customers but is understood to concern the same incident.
- 4 ICO press release entitled *Zurich Insurance agrees to improve information security after losing over 46,000 individuals' personal financial information* dated 24 March 2010 (see http://www.ico.gov.uk/upload/documents/pressreleases/2010/zurich_insurance_plc_240310.pdf).
- 5 ICO publication entitled *Consultation on the Assessment Notices Code of Practice* dated 10 February 2010 (see http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/consultation_assessment_notices_code_of_practice_20120209.pdf).
- 6 ICO press release entitled *ICO launches new consultation on auditing notices* dated 12 February 2010 (see http://www.ico.gov.uk/upload/documents/pressreleases/2010/assessment_notices_cop_120210.pdf).
- 7 ICO publication entitled *Memorandum submitted by the Information Commissioner to the Public Bill Committee* dated 30 January 2009 (see http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cj_bill_ic_memo_300109.pdf).
- 8 ICO publication entitled *Coroners and Justice Bill: Information Commissioner's commentary on the Data Protection Clauses (151 – 154 & Sch.18)* dated 13 February 2009 (see http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_commentary_170209.pdf).

- 9 ICO publication entitled *Commentary from the Information Commissioner's Office – House of Lords 2nd Reading* dated 18 May 2009 (see http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cj_bill_lords_2nd_reading_v2%200.pdf).
- 10 See, for example, the ICO press release entitled *ICO launches new consultation on auditing notices* dated 12 February 2010 (see http://www.ico.gov.uk/upload/documents/pressreleases/2010/assessment_notices_cop_120210.pdf).
- 11 ICO guidance entitled *Information Commissioner's guidance about the issue of monetary penalties prepared and issued under section 55C (1) of the Data Protection Act 1998* dated 12 January 2010 (see http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/ico_guidance_monetary_penalties.pdf).
- 12 BBC News articles entitled *HSBC fined for personal data loss* dated 22 July 2009 (see <http://news.bbc.co.uk/1/hi/business/8162787.stm>).