
UNITED KINGDOM NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

# Mandatory audits for private sector firms on the horizon

Amendments to the Coroners and Justice Bill may make certain private sector data controllers liable for assessment notices. **Mark Young** explains.

Following sustained lobbying by the Information Commissioner's Office (ICO), Government amendments to the Coroners and Justice Bill were passed before the summer recess that introduce a mechanism to empower the ICO to audit certain types of private sector data controllers. As everyone in the data protection community is aware, the ICO has long been calling for enhanced resources and enforcement powers. The progress and content of this Bill indicate that some of these calls are slowly being met. This overview, which explains the data protection elements of this controversial Bill, and specifically the new Assessment Notice regime, serves as a warning for certain private sector companies that a letter and visit from the ICO to assess data protection compliance may soon become a reality.

## The content of the Bill

The Coroners and Justice Bill was introduced in the House of Commons on 14 January 2009. It covers a curiously broad range of issues, including coroners; murder, infanticide and suicide; prohibited images of children; hatred against persons on grounds of sexual orientation; criminal evidence, investigations and procedure; sentencing; and legal aid. It also contains provisions regarding data protection. The Bill would amend over 50 Acts of Parliament, one of which is the Data Protection Act 1998 (the DPA). Unsurprisingly, significant concerns have been raised on a number of occasions about such disparate matters being covered in one Bill rather than being addressed in more specific separate bills. Equally unsurprising is that the Bill has had a rather long and complicated passage through Parliament, and that some of the more politically sensitive issues – such as excluding juries from certain inquests and sentencing – have obtained greater press coverage than the data protection elements. That said, this should not detract from the significance for data controllers of the envisaged amendments to the DPA, as the ICO has been successful in galvanising support for increased powers of audit and is on the verge of being granted important new powers.

## The data protection aspects of the Bill

Following the flurry of reports and consultation papers published in the summer of 2008 on the use of personal data in the public and private sectors and on the ICO's inspection powers and funding arrangements, the government moved to remove barriers to data sharing to support public services and to confer stronger inspection powers on the Information Commissioner. Part 8 of the Bill contains a number of amendments to the DPA, including ex- tending the inspection and audit powers of the Information

*Continued on p.3*

Issue 45 **OCTOBER 2009**

*Mandatory audits... continued from p.1*

Commissioner via a regime of Assessment Notices. It also introduces provisions designed to increase the funding of the ICO through tiered notification fees, in order to provide the additional re-sources that the greater inspection and audit powers would require (p.16). Although the original version of the Bill contained provisions relating to the sharing of personal data across government departments, these were dropped in the face of substantial opposition in Parliament.

## Assessment Notices

The original Section 151 (now Section 162) of the Bill is intended to introduce Assessment Notices (via a new Section 41A of the DPA) that would permit the ICO to inspect data controllers to determine whether they are complying with the data protection principles under the DPA. In short, this procedure would require data controllers to submit to an audit. This is to be contrasted with the current procedure, whereby assessments under Section 51(7) DPA can only be conducted with the consent of the data controller.

Under the new regime, an Assessment Notice would require a data controller to, among other things, permit the ICO to enter any specified premises; inspect any documents, information or materials on the premises to which the ICO is directed (or assisted to view using equipment on the premises); comply with requests for copies of any documents or copies of such documents, information or material; and permit the Commissioner to observe the processing of any personal data that takes place on the premises (Section 41A (3)).

Although Assessment Notices would be served on data controllers, they also could require data controllers to make available for interview by the ICO "a specified number of persons of a specified description who process personal data on behalf of the data controller (or such number as are willing to be interviewed)" (Section 41A(3)(h)).

The Assessment Notice must specify either the time when, or the period within which, the requirements of the notice must be complied with (Section 41A(5)). This must allow time for an appeal to be brought, which effectively means that the need to comply with an Assessment Notice would be suspended in the event of an appeal (Section 41A(7)). In exceptional circumstances, the Information Commissioner could ask the data controller to comply with a requirement in an Assessment Notice as a matter of urgency (Section 47A(8)). Finally, the Bill would also require the Information Commissioner to prepare and issue a code of practice about Assessment Notices.

## Assessment Notices restricted to public sector – the lobbying begins

When it was first published, the Bill only granted the Information Commissioner the power to serve an Assessment Notice on data controllers who were either "a government department" or "a public authority designated . . . by an order made by the Secretary of State". The government had indicated previously that it was conscious of imposing further burdens on business and now maintained that the Information Commissioner had adequate powers to deal with the private sector and that the new assessment powers were designed principally to raise awareness in the public sector. The government argued that the public sector holds significant amounts of data, the processing of which is often necessary to safeguard rights and responsibilities, and – in contrast to the private sector – individuals have no choice over whether such data are processed.

The ICO objected to this restriction based on the level of risk and the many examples of personal data being mishandled in the private sector, and the line of demarcation between the public and other sectors becoming increasingly blurred. In a memorandum submitted to the Public Bill Committee, the ICO stated that it was "strongly of the view that if individuals are to be protected properly, we must be able to serve Assessment Notices on all data controllers – including private sector, public sector and third sector organisations". The ICO also commented that it was "very worrying that the Bill does not provide for any sanction if an Assessment Notice isn't complied with, but does provide for a formal right of appeal against a notice".

In a similar vein, the Joint Committee on Human Rights criticised the government's approach as underestimating the role that the private sector increasingly plays in the processing of information, and the impact that such processing has on the private lives of individuals, particularly when private sector providers deliver public services. The Committee therefore recommended that the government reconsider the ICO's request that the proposed power to issue Assessment Notices be extended to private sector data controllers.

The CBI meanwhile wrote to the members of the Public Bill Committee to express its view that the new powers of assessment provided in the Bill should not be extended to the private sector. The lobbying had begun in earnest.

## First attempts to broaden the scope of Assessment Notices to the private sector

In line with the ICO objections, several amendments were moved at the Committee Stage of the Bill in the House of Commons to extend the scope of Assessment Notices to the private sector and to introduce sanctions for non-compliance. These were subsequently withdrawn, however, with the government stating that this would amount to an "unwarranted extension" of the scheme, which would overburden the private sector in conflict with the Hampton principles (a reference to Sir Philip Hampton's 2005 review, *Reducing administrative burdens: effective inspection and enforcement*). The government at least provided undertakings to consider the scope of the regime further, specifically regarding private sector organisations operating under a contract with a public authority to carry out functions of the latter.

## Second attempt to broaden the scope of Assessment Notices to the private sector

The Bill completed its passage through the Commons and went to the House of Lords at the end of March.

Before second reading took place in

the House of Lords, the ICO again commented on what it described as "two fundamental weaknesses" in the envisaged Assessment Notice procedure, namely that the notices did not extend to the private sector, and that the Bill did not provide an effective mechanism for sanctioning failure to meet a requirement of a notice. The ICO stated that it has long argued that requiring an organisation's agreement before the ICO can inspect it to check whether it is complying with the data protection principles is unacceptable for effective regulation, and that this concern had been shared by various Select Committees and enunciated in recent data protection reviews and reports. The ICO repeated that considerable data risks can arise outside the public sector, drawing particular attention to commercial online activity where companies hold repositories of information derived from customers' activities and interests, financial institutions and credit reference agencies, and retailers' loyalty card databases.

The government appeared to back down at this stage, and agreed to introduce provisions that would extend the ICO's audit powers to classes of data controllers without creating a disproportionate regulatory burden. Relevant amendments were duly moved at the Committee Stage in the House of Lords.

## The mechanism for empowering the ICO to audit private companies

Out of concern for protecting private companies from undue interference, the government amendments and current version of the Bill would not extend the procedure automatically to all private sector data controllers. Instead, they would allow the Secretary of State to designate by order certain descriptions of private sector data controllers liable for Assessment Notices, following a recommendation from the Information Commissioner. If the Secretary of State accepts such a recommendation, the affected sectors would be consulted before any order is made. Such consultations would be accompanied by a full impact assessment. The Secretary of State and the Information Commissioner would have to be satisfied that designation is necessary, taking into account the nature and quantity of data under the control of such persons, and the damage or distress that may be caused by a contravention by such persons of the data protection principles.

As Lord Bach made clear for the government during the Committee Stage in the Lords, this amendment does not provide for the designation of a particular data controller but for a description of a data controller. This means that the designation would not single out or list individual data controllers but would provide a description of a class of data controller – for example, credit reference agencies – as liable to Assessment Notices. The government amendments would require the Secretary of State to review, at least every five years, whether it continues to be necessary for a description of a private sector data controller to be subject to the Assessment Notice regime.

Further government amendments introduce changes that provide the ICO with the power to apply for a warrant under Schedule 9 of the DPA where a data controller fails to comply with a requirement imposed by an Assessment Notice. As is the case currently, the ICO would need to satisfy the judge that there were sufficient grounds for the issue of a warrant to search the data controller's premises. The government contended that the key difficulty with treating the failure to comply with an Assessment Notice as a contempt of court or as an offence – alternative solutions suggested at various stages during the progress of the Bill – is that ultimately it would not provide the ICO with access to the premises in question, which is what a warrant provides.

Clearly this is quite a cautious approach to introducing an audit regime to private sector companies. The ICO has stated that "the process for designating a 'description of the persons' subject to the Assessment Notice power must be effective" and warned that while "those likely to be affected by any designation should be consulted … the new inspection regime will not get off the ground if the designation process is overly bureaucratic or time-consuming, or if the Information Commissioner's initial recommendation is not given due weight".

## Next steps and the likely risk of an audit

Having completed the first and second readings and the Committee Stage in the House of Lords, the Bill has now moved to Report Stage for further examination. This is scheduled to take place on 21, 26 and 28 October. This will give all Members of the Lords further opportunity to consider amendments to the Bill. It will then move to third reading for the final chance for the Lords to debate and amend the Bill. As the Bill started in the House of Commons, after third reading in the Lords, the amended Bill will be sent back to the Commons for it to consider the Lords amendments. There then follows the stage known as ping-pong, where the Bill may go back and forth between each House until both Houses reach agreement.

There may therefore be further twists and turns regarding this Bill and the content of the Assessment Notice provisions, but the government is determined to complete the Bill's progress through Parliament and for it to be enacted as soon as possible following the summer recess. The current parliamentary term expires in November, so there is little time to spare if the Bill is to become law.

If the Bill passes, it is unlikely to bring about a widespread auditing regime in the UK, as the ICO simply does not have the resources to be traversing the country auditing the practices of over 300,000 data controllers. As the ICO explained in a memorandum on the government amendments introduced in the House of Lords, "even with the additional resources we expect to receive from tiered [notification] fees, we only expect to conduct around 100 assessments per year across all sectors. . . If our power to issue Assessment Notices is extended to the private sector the likelihood of the average business receiving a notice in any one year is slight, unless their processing poses a real and significant risk to individuals."

Companies should not be complacent, however. The ICO has welcomed the proposals in the government's amendment and believes these should provide the foundations on which to

build an effective inspection regime for the ICO. It also has reserved its right to return to this issue in the future in the light of experience of operating the system as proposed. Even if the Bill fails, efforts to introduce an Assessment Notice regime and to empower the ICO to audit private companies are likely to continue, even if there is a change of government following next year's General Election. The Tories recently have committed to strengthen the audit powers and independence of the Information Commissioner as part of what they state will be a fundamentally different approach to protecting personal data and personal privacy in the UK. Companies that could be potential targets for audits by the ICO should therefore remain alert to these developments, and if the proposed regime under the Bill becomes law, start thinking about how to prepare for receiving a notice and subsequent visit from the Commissioner.

**AUTHOR**

Mark Young is an Associate in the Data Privacy and Security Practice of Covington & Burling LLP
Email: myoung@cov.com