

CORONERS AND JUSTICE BILL – CLAUSE 156

Memorandum submitted by the Information Commissioner on Government amendments introduced in the House of Lords – July 2009.

The Information Commissioner is content that the Government amendments will open the way to a more effective data protection inspection regime, providing better protection for individuals against organisations whose activities pose a particular risk, and improving public trust and confidence in the processing of personal data.

The Commissioner believes that it would be helpful to explain how the assessment process works:

- The ICO decides to carry out an assessment where it appears that there is a particular risk to individuals or suspicion of non-compliance, e.g. where a large number of sensitive records are held, or where a series of complaints have been received. This risk-based approach is in line with the principles of regulatory good practice.
- An assessment of a larger organisation typically involves three or four ICO auditors visiting for three or four days and interviewing 12-30 staff. We usually focus on a particular aspect of an organisation's activity, e.g. its security procedures, leaving other parts unaffected. Most assessments involve larger organisations. Where smaller organisations are involved, the scale of the operation (and hence the burden) is considerably reduced.
- After an assessment, an organisation found lacking receives good practice recommendations. Our constructive feedback helps organisations to improve standards and, in most cases, reduces the likelihood of more formal action in the future. Only where there is evidence of a serious contravention, and the organisation fails to respond appropriately, will we issue an enforcement notice.
- We work with organisations in a spirit of co-operation including agreeing the time, place and scope of any assessment. We intend to continue on this basis. However, there must be a fall-back position in which we can carry out checks on organisations whose activities pose a particular risk to individuals, but who will not co-operate with us voluntarily.
- We already have a formal agreement with the Government on detailed arrangements for 'spot-checks' on Government departments. This makes clear what departments can reasonably expect and provide safeguards. The proposed statutory code of practice will provide a similar level of transparency and safeguards for all organisations subject to assessment notices.
- The number of assessments undertaken is primarily dependent on the ICO's resources and will not change significantly as a result of strengthening of our powers. However, new powers will make our assessments more effective, through better targeting and less time wasted negotiating entry. They will also help us to target areas of risk, leaving the majority of low-risk organisations alone. For many organisations, the existence of the powers would be a powerful spur to compliance, whether or not they need to be deployed.

Even with the additional resources we expect to receive from tiered fees, we only expect to conduct around 100 assessments per year across all sectors. This is out of a population of over 317,000 notified data controllers. 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.

The level of risk that arises in the private sector should not be underestimated. There have been many examples of mishandling. In addition, the line of demarcation between the public and other sectors is becoming blurred. Private and third sector bodies frequently carry out work for public sector ones. It is common for charities, for example, to carry out functions on behalf of local government. As the Bill stands unamended, we would be able to inspect the local authority, but not the charity.

Some private sector bodies have collections of sensitive information that are as extensive as those held within the public sector. In reality, an individual may have no alternative to providing information to a private sector body, for example to a bank or credit reference agency. The loss or misuse of private sector information can have an enormously detrimental effect.

If the necessary improvements to the ICO's inspection powers are to be achieved, the process for designating a 'description of the persons' subject to the assessment notice power must be effective. We recognise that those likely to be affected by any designation should be consulted, but 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.

The House of Lords Select Committee on the Constitution, in its report on 'Surveillance, Citizens and the State', February 2009, supported the need for an assessment notice power covering private sector organisations:

"[We] regret the decision not to legislate for a comparable [inspection] power with respect to private sector organisations. We recommend that the Government reconsider this matter. Organisations which refuse to allow the Commissioner to carry out inspections are likely to be those with something to hide."

There remains a strong case for an assessment notice power that applies to all organisations subject to the Data Protection Act 1998 without the need for further designation through secondary legislation. Nevertheless, we welcome even the more limited proposals in the Government's amendment and believe these should provide the foundations on which to build an effective inspection regime for the ICO. We reserve the right to return to this issue in the future in the light of experience operating the system as proposed.

Christopher Graham
Information Commissioner

13 July 2009