Impact of the EU Data Protection Directive in the UK

What impact will the EU Data Protection Directive have in changing the familiar UK Data Protection Act? Anne Hinde, Senior Policy Adviser at the Office of the UK Data Protection Registrar, explains.

Many people will have seen, and obtained their copy of the Registrar's submission to the Home Office Consultation Paper, entitled *Our Answers* (July 1996). There is a more recent document, *EC Data Protection Directive 95/46/EC: Preparing for Implementation (June 1997)* available on the Registrar's website: http://www.open.gov.uk/dpr/dprhome.htm. But this comes with a clear "health warning" since it is difficult to be too specific in the absence of published policy from the Home Office /Government, and, indeed, the legislation itself.

Context of implementation

We welcome the fact that implementation will be through primary legislation, giving a seamless regime across all sectors. It will also give the opportunity to modernise data protection law.

The reference to Data Protection primary legislation in the Queen's speech (at the opening of the current session of Parliament) was in the context of open and transparent Government. The main strands of this are to be:

- greater use of information technology for the public to better access Government services;
- the Government's Freedom of Information (FOI) proposals; and
- the incorporation of the European Convention on Human Rights (ECHR) into UK law.

The first of these requires public confidence in the processing of data, which could be based on a sound data protection regime, with compliance and monitoring of such compliance.

The second will have implications for Data Protection, especially where personal information is included in the public record as disclosed under FOI legislation.

The incorporation of the ECHR is relevant in that it was one of the original roots of Data Protection legislation.

Privacy issues

The emphasis on personal privacy related to the processing of personal data is new for the UK, although it is specifically spelt out in Article 1.1 of the EU Directive, which the Registrar would specifically like to see incorporated into the new Data Protection Act.

The Registrar's current mission statement already emphasises the privacy aspects of the Registrar's work, but it would be helpful to have this in the legislation as well.

The Registrar suggests that data users looking to the future should ask themselves whether their intended processing operations will satisfy the first objective of the Directive.

Data users' new responsibilities

There are five main areas where the Directive will have an impact.

1. Scope: Data users will need to determine whether they are within the scope of the legislation. At present, the scope of the UK Data Protection Act covers automatically processed personal data. In the future, there will be a wider definition of processing, to include some manual records.

2. Registration: If data processing is within the Directive's scope, then data users need to register (unless within narrow exemptions). At present, all data users need to register, called *notification* in the Directive. In the future, there will be a tiered system based on risk assessment.

- Some users may not need to notify if their processes are of low risk category, or a *simplified standardised notification* system may be sufficient;
- others will need to *notify some details* of their processing, much as at present;
- for very few of the most sensitive processing operations there will be the need for *prior checking* before processing is allowed;
- The current changes the Registrar is making to Registration are based on the Directive's requirements. Data users will need, as always, to be fully conversant with the range and nature of the data processing that takes place to see whether they will come within one of the exemptions, or into which risk/notification categories they fall;

- The current links between registration and offences will need to be removed.

3. The principles: Data users will need to comply with the eight data protection principles. At present, the Data Protection Act has eight data protection principles. In the future, similar principles appear (scattered) in the Directive, but data controllers still have to comply with the principles regardless of whether they are exempt from, or subject to simplified notification procedures.

Some of the Directive's Articles could be seen as elaboration or interpretation of the recast eight data protection principles.

Enforcement notices are a satisfactory way to ensure data users/controllers comply with the principles.

4. Legitimacy of Processing: This provision applies to all controllers, who could usefully start *now* by thinking about which criteria they will be using to justify the legitimacy of their processing of personal data under Article 7. Controllers may rely on Article 7 (e), "processing is necessary for the performance of a task carried out in the public interest...." or Article 7 (f) "processing is necessary for the purposes of the legitimate interests pursued by the controller....." If so, then Article 14 (a) may apply which gives data subjects a new right to object to their data being processed "on compelling legitimate grounds relating to an individual's situation".

5. Sensitive Data: The special categories for which the Directive prohibits additional and restrictive rules (Article 8 Paragraph 1) are personal data revealing: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade-union membership; and the processing of data regarding health or sex life.

The existing 1984 Act provides for the Secretary of State to make an Order which can modify or supplement the Data Protection principles to provide additional safeguards when processing "sensitive data" (as defined in the 1984 Act - which does not include the category of Trade Union membership). There will have to be special rules for processing sensitive data after the Directive comes into force. The Directive assumes that processing sensitive data is prohibited unless certain exemptions apply. Many of these Article 8 exemptions (which allow the processing of sensitive data under certain conditions) contain references to "adequate safeguards". The Registrar's publication, *Our Answers,* suggests that the details of such safeguards could be determined by reference to the particular processing operation. In our view, these should generally include:

1. strict prohibitions and restrictions on further use and disclosure of special categories of personal data;
2. notification to the data subject of appropriate details of the processing operation; and,
3. where appropriate, using Privacy Enhancing Technologies, for example, to pseudonymise personal data.

This is another area where forward planning might pay off.

Data users should, therefore, be asking themselves on what grounds will their processing of sensitive data take place? If they cannot establish grounds, then they need to ask themselves whether they could justify asking for an exemption on grounds of substantial public interest under Article 8 (4).

6. Transborder Data Flows: There will be new rules and restrictions, especially concerning the adequacy of protection likely to be present in the receiving country (Articles 25 & 26).

Data subjects' rights extended

Under the current UK law, data subjects have rights to:

- *access* their personal data,
- have *inaccurate data corrected or erased*,
- (limited rights) to claim *compensation* through the courts when they have suffered damage due to inaccurate data, from loss, or from unauthorised disclosure of personal data.

Individuals may also *complain* to the Registrar about breaches of the Principles or other provisions of the Act.

Under the Directive, the data subject has extensions of these rights.

1. Extended rights: There is an enhanced *subject access right* (Article 12) to obtain information about the processing including sources of the data (if available) and knowledge of the logic in the

automatic processing of any personal data, at least in the cases of Article 15. Article 15 paragraph 1 states that individuals shall not be subject to *automated individual decisions*, although it is not clear what information needs to be provided to satisfy this provision.

It is possible that technologies, such as a secure smart-card reader, may be acceptable, in place of hard copy information which is currently the usual way of providing individuals with a copy of their own information.

Under Article 12, an individual not only has a right to have *inaccurate or incomplete information corrected or erased* but also blocked if the processing does not comply with the Directive. There is also the need to tell any people to whom the data has been disclosed, if such action is taken, unless this involves undue effort. Again, this may cause data users to look at their systems to see if they could cope with such a provision now, and if not, what steps are they going to take to enable them to do so.

2. Compensation and complaints: The compensation provisions in the Directive are wider than those in the present legislation, although there is a defence for controllers to prove that they are not responsible for the event giving rise to the damage. *Our Answers* suggested that damages should be available from any person at fault. When assessing the risks from any processing operation, it would be worth remembering the possibility that any unlawful processing operation resulting in damage to the data subject may lead to a claim for compensation once the new law is in place.

Under the 1984 Act, the Registrar has to consider *complaints* about breaches of the Data Protection principles or breaches of any provisions of the Act. Under the Directive, the Supervisory body can also receive complaints from individuals about breaches of their rights and freedoms, and in addition, make *checks on the lawfulness of processing*. This is even more likely when a Data User/Controller relies on an exemption.

3. New rights: There are also some new rights for data subjects - each of which also has some exemptions.

1. For personal data used for *direct marketing*, there is a new right to object to processing (Article 14 (b)),
2. There is a right not to be subject to automated individual decision making, except in some specific cases (Article 15.1),
3. There is the right to be informed of processing, and
4. to legitimise some processing by informed consent.

New powers for the supervisory authority?

Article 28 paragraph 3 provides that the supervisory authority shall have investigatory powers, and gives examples such as:

"... the power of access to data forming the subject matter of processing operations, and the power to collect all information necessary for the performance of its supervisory duties."

The Registrar would like to see three new powers given to the new supervisory body.

1. Information notice: The Registrar would like the power to serve a formal *Information Notice*.

Currently, the Registrar has no express powers of investigation, and the Act does not contain powers requiring individuals to provide information to the Registrar's investigators. We have suggested that the supervisory authority should be provided with the formal power to serve an Information Notice on any person. This would require that individual to provide the supervisory authority with information specified in the notice.

2. Codes of conduct: The Directive provides (Article 27) that the supervisory authority should give an *opinion on Codes of Conduct* submitted to it. Such Codes of Conduct/Codes of Practice are valuable in that they can provide a flexible and appropriate means of applying general Data Protection principles to specific circumstances, technologies or particular sectors. By setting out clearly and publicly what is required of particular controllers, Codes of Conduct can not only assist data user's/controller's compliance, but they can also provide a useful means of developing data subjects' confidence in the way their personal data is being processed.

Our Answers proposes that the supervisory authority should be given the power not only to provide an opinion on Codes of Conduct, as required by the Directive, but also the power to

initiate and develop Codes in particular circumstances, such as where the use of a new technology raises special issues. The process by which the code might be developed should be set in the legislation. This would provide for a formal consultation period and a means of formal adoption. Thereafter, such codes would be enforceable. The Directive does not, as such, require that codes be initiated, developed or enforced by the supervisory body. The Registrar would be interested in feedback on this issue, and on the next proposal.

3. Quality Assurance: The third power proposed by the Registrar is the *power to undertake quality assurance studies*. We are in an increasingly complex Information Society, with ever more sophisticated information handling and communication systems. If people are to use these systems willingly they have to have confidence that their personal data is being properly handled. In our view, data protection is as much about developing an information - handling culture that recognises the value and privacy of personal data, as it is about direct compliance with the Act itself. It is about setting and ensuring high standards of information handling.

> "..data protection is as much about developing an information handling culture that recognises the value and privacy of personal data as it is about direct compliance with the Act itself"

We believe that it would be helpful if the supervisory authority be given the power to undertake a quality assurance type of study or review of processing operations, where there are no concerns that would give rise to investigative powers. The purpose would be to:

1. give the supervisory authority greater understanding of the world of personal data handling
2. use the results to develop best practice; to promote that practice and
3. raise awareness and to give confidence to the citizen.

This is not a power required by the need to implement the Directive, but we see it as a power required by the need to respond appropriately and positively to the fast moving world of electronic information.

Welcoming the Directive

In welcoming the implementation of the Directive by a new Data Protection Bill, the Registrar said, "I am confident that this Bill can provide an opportunity for a new, flexible Data Protection Law for the twenty-first century. The UK can now do more than just implement the 1995 Data Protection Directive. I am pleased that the Government sees data protection as part of the commitment to open and transparent government. The new law can give guarantees to the public that their privacy will be respected in the Information Age."

I look forward with great interest to the Government's proposals for new Data Protection legislation which I hope will be published sooner rather than later.

CCTV surveillance - is it to be regulated?

Among the questions asked afterwards, Michael Spencer (European consultant on civil liberties) asked whether CCTV surveillance, currently largely unregulated, was to be covered by the new legislation. The current 1984 Act already provided some coverage, depending on how the records are accessed. Graham Sutton of the Home Office added that the new Directive has a wider definition of processing, specifically including sounds and pictures, and will not, unlike the 1984 Act, apply only to cases where a recording is made as opposed to a CCTV picture with no recording made. It may be that if the state is undertaking criminal surveillance, it is outside community law, and it might be that the Directive would not apply anyway. One would need to see the details of the legislation.

Presented by Anne Hinde, Senior Policy Adviser, UK Office of the Data Protection Registrar, at the *Privacy Laws & Business* 10th Annual Conference, July 1997. Reported by Robert Waixel, Lecturer, Computer Science, Anglia Polytechnic University, Cambridge. E-mail: rwaixell@csd.anglia.ac.uk