IMPACT OF EU DIRECTIVE ON THE DEVELOPMENT AND INTERPRETATION OF THE UK DP ACT

Once adopted, the Directive has to be implemented by national legislation. Normally, this transitional period is 2 years, hence the new UK legislation is unlikely to come into force before late 1997. However, there will be changes to the UK law. To help organisations plan ahead, Francis Aldhouse, the UK's Deputy Data Protection Registrar here identifies 11 areas where changes are likely to occur and answers questions.

Impact of the Directive on the UK's Data Protection Act

On the question of interpretation and development of the UK legislation, the European Commission has certain powers against a Member State which fails to implement a directive, or passes legislation in breach of the Directive. The ultimate remedy is an action before the European Court of Justice and extensive jurisprudence has already been tested in many cases before the Court in Luxembourg. However, there are still some ambiguities as to the way in which some of the provisions should be transposed in national law. For example, if the UK's Data Protection Act (DPA) were not changed, would the directive's right of a data subject to object to processing on legitimate grounds lead to a new interpretation of the DPA and a new right of action before the UK courts? For example, would it be possible to bring an action for breach of principles under the DPA?

A Directive, as a legal instrument, is supposed to set a legal framework within which a particular issue should be regulated by Member States in accordance with their national legal circumstances and environment. Thus, Member States have a legal obligation to implement the Directive in their national legal systems at a minimum level set by the Directive. This particular Data Protection Directive allows a fair amount of scope to Member States for transposing its provisions into national law. However, it is still being debated whether the Directive would allow implementation at a stricter level. It seems that it will be possible to envisage an even higher level of protection in national law, provided that this has no restrictive effects on data flows within the EU.

Since the Directive applies only to areas within EU competence, the question arises how other non-EU areas, such as police, should be regulated at national level. Should there be one law implementing the Directive for areas within EU jurisdiction, and other laws for other areas? This is not clear yet, especially since the concept and limits of EU competence is constantly changing and expanding. The traditional view within the UK is that it is preferable to have one data protection law for all areas. There is a possibility that the Directive could be implemented by an Order under the European Communities Act.

The Directive will undoubtedly bring some changes to the present UK Data Protection Act. However, there is no need for great concern, since for most organisations everyday data protection practices should remain more or less the same.

The main areas of change

1. Registration

At present, in the UK, registration is a dominant element of data protection for most organisations. For a great number of data users, data protection is all about how to register and avoid problems. The Directive will bring some radical changes in the registration system by simplifying and exempting certain categories of data processing from the notification requirement.

The final result might be similar to the French system of simplified rules established for the most common sectors and types of processing which do not manifestly infringe data subjects' right of privacy; organisations have only to make a simplified declaration of

conforming with these rules. The Data Protection Registrar has been asking for a simplified system since 1989. Under the Registrar's 1989 proposals, registration would be confined to about a third of those who have to register at present. All those exempt from registration would still have to comply with the Principles. It would enable the Data Protection Registrar to concentrate on the major issues, as proposed by the National Audit Office's 1993 report.

2. Enforcement

The Directive will give some additional powers to the Data Protection Registrar which do not feature in the UK Act. Thus, the Registrar will have powers of inspection and audit, as well as the right to demand and obtain information from a data user. But it is likely that the Registrar's approach will remain one of discussion before formal enforcement action.

3. The principle of fair obtaining of personal data

The present draft of the Directive (Art. 11) envisages that when collecting data from a data subject, the data controller has to inform the latter of the following:

- the purpose of the processing
- the obligatory or voluntary nature of any replies and the consequences of a failure to reply
- the recipients of the data
- his right of access to and rectification of the data
- the identity of the data controller.

Although the Directive does not state explicitly the time at which this information has to be provided to a data subject, on the basis of interpreting the spirit of its provision this should be done at the time of collection or before. This interpretation is consistent with the UK law as established in the recent Innovations case (September 1993). The Data Protection Tribunal interpreted the principle of fair obtaining of data to mean that a data subject should be given at the time of collection basic information as to the purpose of processing, the identity of the data user and any non-obvious uses of personal data collected.

However, the direct marketing industry, represented at European level by FEDIM, lobbied heavily for a change to what is now Art. 11 of the Directive, which would allow a data controller to provide the necessary information at a later stage.

4. Sensitive data

Although at first glance the Directive seems to contain an absolute prohibition on processing sensitive data (Art. 8), there are a number of exceptions to this rule. A general basis for exemption is the written express consent of a data subject to processing of his sensitive data. Concerning the definition of sensitive data, the conventional listing contained in the Council of Europe Convention 108 has been repeated in the Directive, with the addition of data revealing trade union membership.

A problem is the use of health data for medical research purposes. There should be no legal difference whether treatment is offered in the public or private sectors. The Data Protection Registrar's view is that if one presents oneself for medical treatment, the information obtained in the course of that treatment is subject to a duty of confidence which prevents the use of that personal data for research purposes.

However, there are some proposals to modify the existing Art. 8 of the Directive to allow for the use of medical treatment data for research purposes.

5. Transborder data flows

The issue of transfers of personal data to countries outside the EU is a complex one. Its resolution is more of a political matter than a legal one.

6. Individual rights

The UK Data Protection Act gives the individual a right of access to his personal data but the right to demand compensation only in limited cases. The Registrar is not aware of any compensation action which has been concluded in the courts. The Directive will

bring the following substantive changes to the rights of data subjects:

- an individual will be given wider scope to bring an action before the courts. This will help to test and establish case law and the courts' interpretation would enable data protection to evolve.
- an individual will have a right to object on legitimate grounds to processing of his personal data (Art. 15).
- there will be a judicial remedy for any breach of individual's rights guaranteed by the Directive, as well as a liability provision giving an individual a right of compensation for damages suffered as a result of any act incompatible with the national legislation implementing the Directive (Art 22).

This means that the individual will be able to go directly to court without having to rely on the Data Protection Registrar bringing a formal action before the courts.

7. Manual data

The distinction between manual data and automated data can be an arbitrary one. Although there are grounds for distinguishing between manual and automatically processed data, the Registrar comes across cases where the distinction in treatment seems hard to justify.

The discussions on manual data being included in the scope of the Directive have so far concluded that the Directive should apply to personal data which is organised and structured in such a manner as to facilitate the access to and use of personal data relating to an individual. This will bring a major change to the present regime under the UK DPA. There will be some practical problems of compliance, especially with the data protection principles and personal data in archives.

8. Data protection principles

The Directive repeats in Art. 6 the basic data protection principles included in the Council of Europe Convention 108 and in the UK DPA. The question arises as to the place this article has within the whole body of the Directive and its relationship with other parts of the Directive. The view of the Registrar and the other Data Protection Commissioners in the EU is that Article 6 as well as the other provisions of Chapter II of the Directive must always be complied with and Article 6 is therefore of overriding importance. The UK DPA is driven by principles and the Data Protection Registrar prefers general principles to prevail as they are more flexible.

9. Definitions

The definitions adopted by the Directive differ from some of those in the UK DPA. Some of these differences in the Directive are:

- "processing" is not necessarily by reference to a data subject.
- in the definition of "personal data" there is no reference to opinions and intentions. The current UK DPA has an exemption for intentions.
- the UK Act refers to "data user", whereas the Directive uses the term "data controller," defined as any natural or legal person who process personal data and decides on: its purpose, its contents, its uses and third parties recipients of this data. A problem arises where more than one body is responsible for deciding on all the above factors, as is the case with a Chief Constable and the Police National Computer, or with electronic publishing. Who is then considered to be the data controller? It has been suggested by some that the issue could be simplified by restricting the definition of controller to a person who controls the purpose of the processing.

10. Exceptions to the right of access

The Directive in Art. 14 lists circumstances in which a data controller may restrict the exercise of a data subject's access right. These are mainly in matters of public interest and public order. The listing follows the one envisaged in Art. 9 of the Council of Europe Convention 108. However, unlike the Convention, the Directive's exceptions are related only to subject access requests and are

not total exemptions from the other provisions of the Directive.

The Registrar considers that it might be valuable to extend the power to derogate given in Article 14 to matters other than subject access, but it is important to provide for a strict and proper test which would justify such an exemption. Thus, a similar test to the one adopted in the Convention 108 - necessity in a democratic society, and restriction to a specific list of purposes - would seem to be a proper basis to qualify for an exemption given by the Directive.

11. Jurisdiction

The question of applicable national law adopted pursuant to the Directive (Art. 4) is still a point of great debate. The current Art. 4 raises great problems in practice. Some of these are: the principles of lawful processing and fair obtaining of data, exercise of subject access rights and enforcement. For example, which law ought to apply when a company established in one Member State collects and processes data in another, and particularly where the data subjects all reside in the latter country?

Questions and discussion

1. Would an individual have a right of compensation against a government for non-compliance?

As established by the case law of the European Court of Justice (ECJ), an EU Directive can have a direct effect against public bodies, which means that an individual may invoke a right given by a Directive in national courts. Also, since the Frankovich decision of the ECJ, an individual may demand compensation in an action against a Member State failing to implement a Directive.

2. By giving exemptions from and simplifying registration, does the Directive go too far in the direction of self-regulation by permitting data controllers to neglect the discipline required by the current UK system of being forced to think about their purposes for holding personal data?

There should be no fear that the system of simplified registration as operated in France would lead to circumvention of legislation and attention being exclusively directed to ensuring that an organisation falls within the prescribed categories. On the contrary, registration will be de-coupled from non compliance with data protection principles. At present, the Data Protection Registrar is limited to supervisory tasks only in relation to registered data users.

3. The Directive's inclusion of manual data will cause practical problems.

Manual data is most probably going to be covered in the directive. Thus, attention should be given to the question of practical compliance. We should concentrate on establishing which manual data falls within the scope of the Directive. It is recognised that there will be problems of compliance, in particular, regarding archives and subject access rights. It might be helpful to have a provision similar to one in the UK DPA allowing for subject access only where the data subject has given the data user the necessary information to locate personal data. However, it can be argued that there is enough scope in the second paragraph of Art. 5 for Member States to allow for such a provision. The Directive leaves it to the Member Sates to more precisely determine the circumstances in which the processing of personal data is lawful.

4. How will the Directive determine who is the data controller of a public database, as the Art. 2 definition of processing includes "consultation and use?" Does this make every user potentially a controller? Does a compiler of a database need permission from each author to list his work?

There is a debate on who ought to count as a data controller. The grey areas include:

1. obtaining information from a published database
2. the compilation of a database
3. consultation of a database.

Consultation of a database does not constitute control of the contents of data and does not make a person consulting it a data user under the current UK law. The Directive seems to put obligations on those who use personal data. The definition of "data controller" has not been finally settled and it is unlikely that it is intended to cover those who merely consult material. Personal data is obtained fairly if an index is going to be compiled on the basis of provided information. However, if the data is used for another purpose then the principle of fair processing has to be tested for the secondary purpose, also.

5. How will the Directive affect existing codes of conduct?

The Directive recognises a place for codes of conduct both on national and EU level. Concerning the national codes of practice, there will be novelties in the process of drawing up these codes. Beside greater formality in general, the national authorities will have powers of vetting and approval.

The UK has some experience with these self-regulatory instruments. The Data Protection Registrar recognises that codes of conduct can be valuable, especially in emphasising and dealing with problems in particular sectors. For example, the Direct Marketing Code of Conduct envisages some very useful instruments, such as a chain of warranty.

However, the Registrar has expressed some anxiety over motives behind bringing forward the codes. Codes of conduct should reflect the details of the sector and give data users more certainty on their use of personal data and not be a route to avoid proper control.

This report is based on a presentation given by Francis Aldhouse, the UK's Deputy Data Protection Registrar at the UK's Data Protection Forum, 9th February 1994. This report was written by Bojana Bellamy, a *Privacy Laws & Business* consultant.