# UK Data Protection Registrar poses questions on the EU Directive's implementation

**Following publication of the Home Office consultation document, the Office of the Data Protection Registrar produced in April this year *Questions to Answer*. The Registrar writes, "This is an opportunity that arises once in fifteen or twenty years to influence legislation." In this report, Francis Aldhouse, Deputy Registrar, explains the questions designed "to stimulate a debate and to encourage as wide-ranging a review of data protection legislation as possible....and provoke a comprehensive response to the Home Office."**

I note with regret that Graham Sutton said that the government's intention was to do the least possible to implement the Directive, and indeed to comply with the 1981 Council of Europe Convention. I take objection to that tone of presentation, which gives the wrong impression and starts the debate with, "Let's do the very least possible."

The Registrar's predecessor in 1989 produced many proposals which did not proceed very far. One of the reasons given was that it would be looked at in due course, when it could be swept up with the review that will follow the adoption of the Directive and its necessary implementation. The Registrar takes the view that this minimal approach is not helpful towards a data protection law that will carry us into the next century.

We have produced a document called *Questions to Answer*, containing twelve key questions.

## 1. Is data protection about personal privacy?

Not much has been said in the UK discussions, and you will not find much in the Home Office document, about data protection as a privacy protection issue. Data protection is more usually presented as a technical issue, raising questions such as how to register, and what other detailed rules those in business have to follow.

Article 1 says it is about protecting the privacy of individuals. But it is not a total privacy law; it does not deal with physical invasions or other matters; it deals only with the proper rules for handling information about individuals. It owes its origin to the 1981 Council of Europe Convention no.108, clearly recognised by the House of Lords, the UK's supreme court, in *R v Brown* as the origin of our data protection legislation and that which gives the privacy protection element to data protection. The 1981 Council of Europe Convention in turn, owes its origin to the European Convention on Human Rights.

So the first question is: do you agree that data protection is about personal privacy? If you read the 1984 Act you would think it was about the regulation of sewage pipes. Should the new law expressly include a reference to the protection of privacy? If we are going to satisfy the Directive in a minimal way, it is only necessary to replicate the effective provisions of the Directive.

## 2. Primary or secondary legislation?

In looking at the issue of whether the Directive should be implemented by primary or secondary legislation, we have the opportunity to review existing legislation, including matters not within the scope of the Directive. Constitutional arrangements differ widely, but normally in this country, Directives are implemented by regulations, which are secondary legislation made under the European Communities Act 1972.

The Registrar puts forward two reasons in favour of primary legislation, a new law:

- The legislation should be reviewed comprehensively

Primary legislation enables the whole issue of privacy for the future to be considered extensively and with proper time for parliamentary debate. We need to consider what is going to work in the year 2015.

- The government's own agenda

This includes clarifying to the citizen what one can expect from a public body, and the means of readily ensuring rights.

On the other side of the coin, there is great scope in the Directive for deregulation - making things easier for business and non-business data users or controllers.

Only primary legislation can bring such disparate matters within the scope of the Directive, and we need one piece of legislation applying to all circumstances.

Problems arise because matters which are within the scope of the Directive are not clearly divisible into those sectors which are defined as coming under the aegis of European Community competence. Those producing the Directive found this distinction such a problem that they actually excluded certain categories from the scope of the Directive, just to be safe. These excluded categories which are activities of the State in:

- criminal law
- foreign affairs and defence
- justice and home affairs.

The Directive can, as a matter of law, apply only to those matters which are within the scope of Community competence. I have two examples of the sort of difficulty that might arise in practice.

**Road accident records**

Let us say that you are the Superintendent of a police force and there is a road traffic incident. Your officers attend this incident and they do the usual things. They arrange for the damaged vehicles to be removed, they call an ambulance and take statements; they prepare their reports. All this, including the copy statements, will go into a modern integrated system covering matters both within Community competence and those which are not. This is a serious road incident, and, as there is the potential of someone being prosecuted, reports are produced for the Crown Prosecution Service (CPS).

This is clearly an activity of the State involved in the criminal law and outside the scope of the Directive.

In practice, you have a solicitor saying that his client was badly injured in this accident and is thinking of suing the person who caused it and would therefore like to have copies of reports and statements of officers. If the Chief Constable says he can have the report, and if the computer produced the same documentation that went to the CPS, then that processing is within the scope of the Directive, because now it concerns civil litigation and not the criminal law. What about the original collection of the data? Every piece of processing is covered either by the Data Protection Act or by the amended Act of the Directive. When these officers attended this incident and took statements and prepared reports, they were doing something that was both inside the scope of the Directive and outside it. It would be covered by both old and new laws.

Is this a trivial point? We do not know entirely what the consequences will be. We are going to find that individuals have different rights with respect to certain information, or processing, even though it is the same information. They are going to have wider rights to compensation under the Directive than they do under the existing legislation. There are extensive exemptions and there are compelling reasons why we want to go down that route, but we cannot extend that relaxation of registration arrangements to public sector areas unless we have primary legislation that brings all these matters within the scope of the new legislation.

**Business records outside the scope of the Directive?**

I have another example relating to business. Income and corporation tax are largely outside the scope of Community competence, unlike Value Added Tax which is partly within Community competence. If you are a business and employ persons, and keep Pay (Tax) As You Earn (PAYE) records as required by the Inland Revenue, that would appear to be an activity outside the scope of Community competence. However, your ordinary business records are within Community competence and therefore covered by the new law. You would want to have an integrated computer system, but a separate set of rules is needed for matters covered by the old Data Protection Act, and another set to deal with matters covered by the new law. A complete and comprehensive Act is needed. It could be primary legislation authorising extended secondary legislation.

## 3. Should registration be decoupled from enforcement?

At the moment registration is knitted into the way we enforce the law, and we can only take enforcement proceedings against people who are registered. There are powers to refuse registration applications on their merits if the Registrar feels the applicant will not comply with the eight principles: the Code of good information handling practice. We could continue to have registration coupled with enforcement, but it would be a good idea to separate the two. Once that occurs, one can more easily exempt people from registration. They will still have to comply with the principles,

but we can relieve them of the bureaucratic burden.

The Registrar's view is that separation of registration and enforcement is a good idea. Let registration serve a specific purpose as an information source, principally about those people handling sensitive data. Registration will then serve a dual purpose of informing both the Registrar and the ordinary citizen about important risky data activities taking place.

## 4. Should the eight data protection principles be retained as a set of broad principles?

Initially, the Data Protection Act was difficult to come to terms with, due to the broadness of the eight principles. We have become very comfortable with those principles and most people have come to understand what they mean in the light of interpretation by the Data Protection Tribunal. The principles have the advantage of flexibility. There is always a trade-off between certainty and flexibility. In areas where we are trying to judge the consequences of actions for individuals, flexibility and the application of broad principles have proved to be valuable in the past, and will be encouraged in the future.

## 5. Is the concept of simplified notification for non-risk processing attractive?

Should the development of risk criteria be left to the supervisory authority? We are trying to produce a scheme which will work under the present law and enable us to identify the more risky activities, on which we believe we should concentrate our efforts, and the less risky which we can look at less frequently, and thus relieve bureaucratic burdens. If we get the model right, it will provide a basis for either simplification of registration under the new law, or indeed, if thought right, extensive exemption. We say the same model can be used for both.

## 6. Does the concept of an in-house controller have any merit in the UK context?

We have been surprised by the reaction from people so far. We thought that there might be some attraction of having in-house data protection officials to take responsibility for compliance and so simplify or gain exemption from notification to the data protection supervisory authority. However, there appears to be some anxiety about the use of this method; a fear that this duty is going to subject the in-house official to a conflict of loyalties. This is an entirely legitimate concern, but there is still some merit in the scheme.

We would like to ensure that organisations are following data protection rules. One way of doing it is by way of internal auditors; another way would be through the development of this system of in-house officials. If relief from some bureaucratic burden were an incentive, that might be a good thing as a matter of public policy, and there must be some merit of at least providing this option in the law.

## 7. Should individuals enforce more of the new law by litigation? Should the supervisory authority have express powers of investigation and audit, and powers to demand information?

We want to see an enforcement model that will work for both public and private sector organisations, and the individual, in ten to twenty years time. The present system is that an individual has a right to complain to the Registrar, and the Registrar has a duty to consider complaints made by a person if made in a timely manner and if an issue of substance has been raised. We are a small organisation and will only take action on issues where we think it is entirely right that we take enforcement action.

Enforcement action is really addressed to putting a system right and is not well tailored to achieving an individual remedy. It does not obtain compensation for an individual. There are certainly cases where the organisation corrects the error, but does not offer any compensation.

There may be benefit in the new extended right to compensation for individuals arising from any breach of the national implementing law. Should we not separate out the rights of individuals so they have the right of going to the small claims courts to solve individual problems? This would allow the Registrar to concentrate on major system problems.

**Registrar's powers of enforcement**

The Registrar's present powers of investigation are almost non-existent. We do not have the power of

health and safety inspectors to insist that someone answer our questions and give us information; or powers of such inspectors to enter premises at any reasonable time. We have an extremely limited power to enter premises by warrant. The Registrar's powers should have been modelled on the Police and Criminal Evidence Act, a straightforward policing power. Instead, we have a power which is inappropriate because a person may welcome us in and still do nothing.

**Distinction between audit and investigative powers**

The enforcement power should be distinguished from audit, as that is a right of inspection, quite independently of whether one is investigating a specific offence or breach of the law. Should the Registrar have the power of a compulsory audit or a voluntary one?

Then there is the question of extended investigative powers, because we have so few powers that we cannot, in some cases, carry out a proper investigation. But there is a balance to be struck here. We would suggest that the Registrar has:

1. some sort of audit power whether of a voluntary or compulsory nature;
2. some form of power to obtain information - perhaps similar to that of the Irish Data Protection Commissioner.

## 8. Should the Data Protection Tribunal be retained? Should individuals have the right to go to the Tribunal?

What is so special about this Tribunal, which meets very rarely? Just because it is called a Tribunal does not mean it works better. With simple compensation cases, one may do far better going to the Small Claims Court.

## 9. Should the right of access be modified to allow more flexibility in the form of response?

We should provide for greater flexibility in the method by which we allow subjects access to their data.

A lot of the debate about manual data seems odd because the principle of giving access to manual data has already been accepted in UK law through the *Access to Personal Files Act; Access to Medical Records* legislation and one of the earlier piece of legislation, the *Consumer Credit Act 1974* giving a right of access to consumer credit files. It would be a better idea to sweep these all up together and provide a consistent means of enforcement for the ordinary citizen which should be brought under the aegis of the supervisory authority.

## 10. Should data protection legislation and freedom of information legislation (open government) be brought together?

One of the government's proposals is that there should be legislation to give a right of access to personal records held by central government, and that would be seen as analogous to the right of subject access under the Data Protection Act. It is likely that the Data Protection Registrar would be the enforcing authority. This legislation is promised but has not actually been submitted to parliament. Data protection legislation and freedom of information are indissolubly linked; they are two sides of the same coin. Privacy protection is a standard exemption for information access for third parties under open government legislation; this is a sensitive political issue which might become electorally significant over the next year.

## 11. What should be the basis for the approach to exemptions?

Do you agree with the Registrar that it should be Article 9(2) of the Council of Europe Convention? This argues for the necessity, in a democratic society, to achieve a specific list of objectives, such as the protection of major public interests; this test is largely reflected in the Directive. There is an argument that the Directive seeks to go further and provide for exemptions on a number of grounds not provided for in the Convention. If that is true, if that extra provision were relied upon, the UK would have to denounce the 1981 Convention. One of the important elements in the list in Article 9(2) (and also found in Article 12 of the Directive) is the provision that there can be exemptions to protect the rights and freedoms of others. That is an authorisation relied upon for exemptions in the 1984 Act. I think that it will have to be examined more extensively in the future.

## 12. What changes are required to data protection legislation in the Information Society?

We currently have the 1984 Act which will still be in force in 1998 after 15 years. Let us think about a law that will be in force in 2015. Information technology growth between now and 2015 is difficult to predict. We can only look at what has happened in the last fifteen years. How can we have a law of sufficient flexibility and comprehensiveness to provide for a similar level of development?

We will be living in a world in which all information about individuals is subject to this law, which says you must have a legal basis for collecting and processing data; that information must be accurate, kept secure and there must be rights of subject access.

What novel exemptions might be required to protect the rights and freedoms of others? Are there not circumstances where an organisation has a right to make private notes and keep them private? The loophole in the past has been that you can write it down in a little book.

We want a set of proper rules for the future. We come across cases, for example, where insurance companies have a note on file of the amount at which a claim might have to be settled. If the claimant then exercises his right of subject access, that enhances his negotiating position. Is that the way we want to conduct business? Does that insurance company not have the right to keep that note, and to keep it private?

**Media Privacy**

One of the really difficult issues is the special exemption rights that might be given to the media. I have been explaining to journalists and editors, that in the modern world, data protection applies to what they do. They should, therefore, be obtaining data fairly. There may be circumstances in which there is a need to protect investigative journalism, freedom of expression, and free speech and that there should be exemptions.

Article 9 of the Data Protection Directive tries to provide the opportunity for special exemptions to protect journalistic activities and artistic and literary expression. But free speech is a right for us all, not just a right for journalists. How can we strike this proper balance? How can we incorporate amendments in the future law which will preserve free speech for us all, and indeed our social representatives, the media, while at the same time recognising proper protection of privacy which the Directive, the Convention and other international legal instruments set out to secure?

## Questions

### Auditing

*Q1. With auditing, you said it was important to strike a balance. One way to strike a balance is not necessarily to give a supervisory authority the power to audit, although I think that would be a good idea, but to give them the power to require an audit be produced by an independent accredited third party. Is that an option that you have discussed? Would it be an option in the UK and one which the Home Office would be prepared to consider giving you?*

**Response - Francis Aldhouse:**

I do not think it is an option that we have thought about much. We have done so in one sense. I have mentioned a relationship with independent auditors, but we have not thought very much about it in the context of the Directive and its implementation. I do not know how it would be received by the Home Office but I am grateful for the suggestion.

**Response - Graham Sutton:**

As to the Home Office response to audit, certainly we are happy to look at any points made to us in response to the consultation paper. I would like to know what a data protection audit would mean.

### Statutory or judicial legislation on privacy?

*Q2. I entirely agree with the need for primary legislation and I would also like to see included within it some general flexible principles relating to a law of privacy. I would like to put a question to Graham Sutton in relation to two judgements by Lord Hoffman and Lord Bingham - two persuasive speeches in which they state they are in support of the development of a law of privacy in the UK and are prepared to see it judge-made if not made by Parliament. In terms of public policy it seems that we have an opportunity to have this law developed by Parliament or to allow it to be developed by Judges. What is Mr Sutton's view on which would be the best formula to adopt?*

**Response - Graham Sutton:**
I think that this takes the debate somewhat beyond the narrow field of data protection. I do not really have a problem with the concept of privacy being written into our law. The UK has already ratified the 1981 Council of Europe Convention on Data Protection which refers to privacy. The wider question which you have addressed is about a general law relating to privacy and it is not one on which I am in a position to comment. The government's position has been made clear in the context of its response to the Calcutt Report and basically that position is: not yet, or not now.

## Post-election changes?

*Q3. The 1997-1998 Parliamentary Session will probably be the first of a new Parliament. I want to know whether Mr Aldhouse believes Her Majesty's Opposition might side more with the Registrar than with Mr Sutton?*

**Response - Francis Aldhouse:**
The Opposition already has a fairly crowded list of ideas for a first session relating to constitutional matters, and would maintain a commitment to freedom of information legislation if they become the next government. Certainly, the election has to be between now and late Spring 1997. The impression I get is that Opposition front bench spokesmen are as conscious of the pressures on parliamentary time as our current ministers, and might need to be persuaded that there is a sufficiently pressing case for primary legislation.

## Developing the concept of fair use of information

*A conference participant's comment:*
*What changes to data protection legislation are required in an information society where all information is automated? We all acknowledge that this is an overriding question if we are to set a menu for the next fifteen years.*

*I would like to suggest that we are not talking about the broader concept of privacy, (though I personally believe that the concept needs developing as the House of Lords has suggested). We are talking about the fair use of personal information, whether automated or not.*

*What we need is a clear civil right to have personal information used fairly about us. That is already in the first data protection principle, and it is in the Directive. The definition of data processing is very broad.*

*In the careful examples which Francis Aldhouse gives, I would like to apply that idea to his last example of the insurance company that has the private note about what the claim is worth. To my mind, we can see that it is fair not to disclose that information. It is fair under the terms of the present Act, because it is a statement of intention, not a statement of a record of information about a person.*

*If we can develop that concept of fair use of information, we may be doing for the law of information as the House of Lords did in 1932 in Donoghue v Stevenson in relation to snails in bottles. From this case, they developed a well-known principle that a manufacturer who puts out a defective product owes a duty of care to the ultimate consumer.*

*In modern circumstances, you can be as much harmed by the unfair use of information as you can by slipping snails into bottles. We really need to move ahead with a clear objective and develop our thinking.*

**Francis Aldhouse, UK Deputy Data Protection Registrar, based his presentation at the *Privacy Laws & Business* 9th Annual Conference in July 1996 on the document *Questions to Answer* which the Data Protection Registrar's office published in April. Also see *Our Answers* published in July. Both available from the ODPR, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, UK.**
**Telephone: 01625 545700 Fax: 01625 524510**
**E-mail: data@wycliffe.demon.co.uk**

**This report was written by Mark Snell, who is currently completing research for a D.Phil at Oxford University, funded by Telecom (Australia) Fund for Social & Policy Research in Telecommunications.**