Helsinki 2.9. 2004/ra

The 26th International Conference on Privacy and Personal Data Protection
Wroclaw, 14.9. 2004

Reijo Aarnio
Data Protection Commissioner
Finland

THE INDIVIDUALS´ AWARENESS OF THE RIGHT TO PRIVACY

1. Introduction: what does data protection mean?

Ladies and Gentlemen,

The Eurobarometer survey published by the European Commission shows that the public's awareness of data protection is alarmingly low in the EU. The Commission has also pointed out in a report issued in conjunction with LF projects that there are considerable gaps in the general awareness of data protection and that online service models need to be revised in terms of data protection. In other words, we have a practical problem at hand.

I will concentrate on discussing *whose responsibility it is* to improve the public's awareness of data protection.

It is important first to define what 'data protection' means. Privacy is very difficult to define as a concept because we all have different ideas of what it is, depending on the situation. Data protection is easier to approach if we keep mind that it is about the right to privacy when our personal data are processed. I would like to stress the word 'right'. Data protection is a right that belongs to every natural person – more precisely, it is a cluster of rights, to speak in ICT terms, made up of the following elements:

1. the right to control and decide how your personal data is processed, or *autonomy in matters of personal data*;
2. the right to know how your personal data is processed. If data subjects do not know who processes their personal data, for what purpose and how, they have no way of exercising their data protection rights;,
3. the right to live your life without undue interference from outside parties. The protection of privacy also includes the protection of confidentiality in all communications. Hence processing personal data should always be regulated by law;
4. the right to be evaluated on the basis of correct and relevant information;

5. the right to know what criteria automatic decision-making systems are based on;
6. the right to trust data security. If data security is compromised, none of the other rights related to data protection can be secured;
7. the right to receive assistance from independent authorities; and
8. the right to be treated in accordance with all other basic rights. Processing personal data in a way that infringes a person's other basic rights cannot be justified in a democracy, unless such procedures are based on law.

We need these rights so that

- our human dignity is respected
- our autonomy is respected
- our honour is respected
- we will not be discriminated against and
- our equality as citizens is secured.

1. Whose job is it?

Public administration and NGOs

Data protection is, in other words, part of our system of basic and human rights. Therefore, we can say that knowing about data protection is part of civic skills. Data protection should be taught in schools and universities, and the public administration should allocate resources to studying and publicising data protection.

Modern society is investing heavily in developing online services, smart card technologies and furthering the use of ICT in general. Young people in particular are learning to use them with ease. Perhaps for the first time in history we have a situation in which the younger generation is 'wiser' than the old. There is the danger that teachers no longer know how to teach children because they are not as well acquainted with new technologies, while the aged and special groups are being sidelined from this development, the goals of which are so eloquently described in the second item in the lists of the data protection directive. Responsibility for keeping the situation under control in a democratic society falls on the public administration.

In Scandinavia, transparency and openness have been part of authorities' activities for centuries. This and the commonly adopted principles of good governance oblige all public officials to inform citizens about their rights – including those related to data protection. In Finland, the statutory duties of the Data Protection Ombudsman include publicity. It is important to acknowledge, however, that the data protection authorities are not the only ones who are duty-bound in this matter. Whereas the aim of data protection is to ensure that Big Brother is not watching any more than necessary, awareness of our data protection rights and the openness of authorities' activities at large will in turn help Little Brother, the citizens, to keep an eye on Big Brother.

Many NGOs serve as watchdogs for basic rights. In my opinion, such civic activities deserve everyone's support. NGOs often have the latest ICT based channels at their

disposal, such as the Internet, allowing for rapid and efficient communications among their members.

Controllers

This takes us to the topic of controller. We have had a project called the "Internet Police" underway for three years now. In this project we go through a certain number of websites and online services every year according to certain selection criteria. This year we have focused on health care and the related services available on the Internet. In case the information provided to a data subject in conjunction with data collection is deficient, we notify the controller of this register through a standard procedure, so that the service provider can take the action needed. The project has yielded good results.

Why are we targeting controllers in particular, and why do we feel a stab of guilt when we find out that awareness of data protection issues is not very good? The answer is simple: controllers are bound by Articles 10 and 11 in the data protection directive to provide data subjects with necessary information. There are very few exceptions to this very comprehensive requirement.

Co-operation with controllers and the organisations they represent is strategically important. Legal grounds for this are provided by at least two concepts in the directive:

- Codes of conduct are an important tool in achieving a high standard of practice in processing personal data. As far as I understand, a code of conduct as a concept implies that the trade association that has drawn them up will also monitor that they are observed within the branch of industry in question That is why drawing up codes of conduct should be encouraged, provided that they include or are appended with the trade association's account of how the observation of the codes is monitored.
- The data protection directive also enables the appointment of in-house data protection supervisors. It is my understanding that in some countries this task has led to a full-blown industry. But do these people know their job? In Finland we are currently devising a training programme for in-house data protection supervisors. The aim of this training is, among other things, to teach data protection staff to demand that the systems under their control are legal and that adequate information is provided to data subjects.

In my opinion, the quality of the processing systems for personal data is always also a legal question, for which senior management is responsible. The lawfulness of their actions is regulated by internal and external inspectors, who should be able to evaluate the standard of information provided.

Media

Data protection and other interests easily conflict. This, as the whole issue of data protection, is very difficult from the point of view of publicity. As we know, the media is often more interested in bad than in good news. Our great challenge is to attract media interest in the undeniably positive aspects of data protection. It is a cause worth fighting for. In Finland The Act on the Openness of Government Activities includes an obligation of all public authorities to draw up and implement a publicity plan and to use the available media in this. In particular, they are obliged to use popular information networks, mainly the Internet.

Technologies

Could technology be useful in increasing public awareness of data protection? I would say yes. For example in Japan, camera phones are required to have a feature which sounds an alert before a picture is taken. Privacy enhancing technologies aim at promoting and securing privacy. PET inherently includes features that increase its users' awareness of privacy protection. This is one of the reasons why I would like to see an increase in the use of PET. I have suggested that mobile phone and system manufacturers introduce an icon for location services which would show on the screen of a mobile phone whenever a locating process is underway.

Conclusion

As public awareness of data protection improves, it is possible and even likely that the number of contacts made to the Data Protection Ombudsman will also increase. This may lead to a shortage of resources and the deterioration of the service. This forecast is something every authority can prepare for by streamlining their activities. It needs to be remembered, however, that the right of citizens to receive good service needs to be secured in all circumstances. Sometimes streamlining activities is not enough. Increasing publicity and demand for it pushes more costs on data protection authorities. This is why the government should ensure adequate human and financial resources to data protection authorities.