Sören Öman*
Protection of Personal Data – But How?

1 Historical background

The right to protection of privacy in connection with processing of personal data is seen as an outflow of the right to respect for private life. The latter right is regarded as a fundamental human right, protected according to several national constitutions and international instruments, most noticeably Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. Since the 1970s special legislation has been developed for the protection of privacy in connection with processing of personal data by automated means (in computers).

The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers. The Act did not contain many material provisions on when and how the data should be processed, or general data protection principles. Instead, the Act required for each computerised personal data register a prior permit from a new data protection authority – the Data Inspection Board. When a permit was given, the Board issued tailor-made conditions for that register.

Several Western European countries followed Sweden's example and in the 1970s adopted special data protection legislation and instituted special data protection authorities. When several countries provided differing restrictions on the processing of personal data in computerised registers, this became a hindrance to international trade. Provision of goods and services across borders requires automated processing of personal data. The need for international harmonisation became evident. Work on international instruments on data protection commenced within OECD and the Council of Europe.

This work resulted in the 1980 OECD recommendation on guidelines governing the protection of privacy and transborder flows of personal data and the 1981 Council of Europe Convention 108 for the protection of individuals with regard to automatic processing of personal data. The aim of those international instruments was twofold: (i) To provide an international standard for the protection of privacy in order (ii) to facilitate international trade through free flow of personal data across borders. The OECD recommendation is a non-binding instrument, while the Council of Europe Convention is binding for those states which have acceded to the Convention.

The Swedish approach with tailor-made conditions for each register could not work in an international environment, due to the absence of any international body to make the conditions and to the drastic increase in the number of computerised registers. Instead, fundamental data protection principles were developed, taking into account the developments in the

---

* *Sören Öman* is a senior legal advisor commissioned by the Swedish government go make a review of the Swedish 1998 Personal Data Act.

other countries which had enacted data protection legislation. As an example Article 5 under the heading “Quality of data” in the Convention could be mentioned:

> Personal data undergoing automatic processing shall be:
>
> a. obtained and processed fairly and lawfully;
> b. stored for specified and legitimate purposes and not used in a way incompatible with those purposes;
> c. adequate, relevant and not excessive in relation to the purposes for which they are stored;
> d. accurate and, where necessary, kept up to date;
> e. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.

The principles contained in the international instruments were not confined to processing of personal data in computerised registers. The principles were instead applicable to more or less all automatic processing of personal data. As soon as a single piece of information relating to an identifiable individual was keyed into a computer, all principles were to be applied. When the principles were developed in the 1970s and early 1980s, this distinction did not have much practical importance. Personal data were processed in computers almost exclusively in the form of traditional registers. Computers at that time, for example, were not used for everyday production or dissemination of text.

In 1995, after some five years of discussion, the European Union adopted a directive on data protection (Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data). The Data Protection Directive draws upon, elaborates and strengthens the principles contained in the Convention. New principles are also introduced, most noticeably an obligation to inform the registered persons about the processing in connection with the collection of personal data. The principles in the Directive cover all automatic processing of personal data and manual processing of such data which form part of a filing system or are intended to form part of a filing system.

The Directive should have been implemented in all Member States not later than in October 1998. A new Personal Data Act, based on and implementing the Directive, entered into force in Sweden at that time (SFS 1998:204). For various reasons, however, many Member States, Sweden among them, have had difficulty in implementing the Directive. France and Ireland, for example, have yet to implement it fully.

2 Data protection principles and the handling of text

The situation has changed radically since the principles in the international instruments – and the Swedish 1998 Personal Data Act – were developed.

A quarter of a century ago, the automatic processing of personal data was almost exclusively conducted in the form of traditional registers by authorities and corporations with large resources. Personal data registers

were instituted after careful deliberations and cost-benefit analysis. The registers were designed and handled by a limited number of persons. A small authority in Sweden could at the beginning of the 1970s lay down conditions for each of the then existent, relatively few registers.

Today, word processing of text, which has not been structured in order to facilitate retrieval of personal data, is one of the most common forms of automatic processing of personal data. Such processing is now being done every day by almost all enterprises, large and small, and by almost all the millions of office employees in Europe. The production of text in computers is now an everyday activity for everybody. The text produced could be for correspondence, for publication on the Internet or for an internal memo or a draft decision. The development of international telecommunications networks, such as the Internet, has made it possible for small corporations and even private persons to publish text internationally at little or no cost. Restrictions for processing of personal data in computers therefore have a more direct and acute implication for the right to freedom of information and expression. It is in this context interesting to note that the three references for a preliminary ruling on the interpretation of the EC Data Protection Directive which until now have been made to the European Court of Justice all concern proceedings resulting in publication of personal data.

When the data protection principles were developed some twenty years ago, the bulk of (the) word processing (of text) was done by non-automatic means and therefore not covered by the principles. But technological development has also moved the everyday production and publication of text into computers. Thus, the scope of application for the principles has been extended to areas for which they were not originally developed. It is interesting to note that the EC Data Protection Directive extends the application of the principles to include manual processing of personal data, but in this case restricts the application to personal data in traditional registers.

Are the data protection principles adequate for the processing of personal data which goes on today when computers have become an everyday tool for everybody and everything?

I think almost everybody will agree that the principles in themselves are by and large as relevant and adequate today as when they were developed some twenty years ago. The principles work well when it comes to automatic processing of large amounts of personal data contained in traditional registers where the data are structured in order to facilitate retrieval of personal data. The principles were developed with such cases in mind. The application of the principles helps to enhance the public's confidence in the processing carried out by state authorities and large corporations such as banks and insurance companies.

But are the principles also adequate for the "new" forms of processing, namely the handling of text which has not been structured in order to facilitate retrieval of personal data? Since each of the data protection principles seems reasonable in itself, I do not think that anybody can with reason argue that the principles are not also adequate per se for the handling of text containing personal data. Who, for example, could argue that personal data in the text should not be adequate and relevant in relation to the purposes for which they are stored? I nevertheless think that we need a modified – simplified – protection for personal data in connection with the handling of text. It is the technological development in the last twenty years,

and the accompanying widespread and diversified use of the technology, which necessitates a modified protection. The principles themselves may well be reasonable, but the strict application of them to the handling of text may not be.

The application of the comprehensive rules derived from the data protection principles is in my opinion not practical, not necessary and too cumbersome for the today commonplace and highly volatile activity of production and other handling of text in computers carried out by virtually every office employee. For every piece of personal data, the data protection principles would require the employee producing the text – for instance an internal memo – to go through all the steps required by the principles: what is the purpose of processing that piece of personal data, is that piece of personal data adequate and relevant in relation to that purpose etc.? In my opinion, it is not reasonable to have such a bureaucracy, nor the expense it entails, for the everyday handling of text. The lion's share of the text handled is probably totally harmless to the persons mentioned in the text. It is therefore hard to understand why bureaucratic, and costly, rules and routines have to be applied to all handling of text just to prevent the few cases where the processing could be harmful. Anyone with the least knowledge about the realities of office work today also realises that any attempt at strictly applying the data protection principles to all processing of personal data in the course of the everyday handling of text would be futile. In fact, I believe that the principles in practice are not, and will never be, strictly applied when it comes to such processing. An overzealous application of the principles on the everyday handling of text would effectively paralyse any organisation.

If the data protection principles are applicable in situations where this is not reasonable, and the principles therefore are not applied in practice, the overall respect for the principles and their acceptance in the society is threatened. In fact, several of the respondents to a recent survey in Sweden believe that the application of the principles every time someone produces text is absurd (Ds 2001:27).

It is well-known that the application of the data protection principles, and the bureaucratic rules and routines derived from them, including the supervision of the application of the rules by a data protection authority, to the publication or other dissemination of text undoubtedly impede the enjoyment of the right to freedom of expression. Due to the new network technology and the widespread use of international telecommunication networks, the conflict between data protection and the right to freedom of expression has become acute. Today, almost anybody can instantly publish text worldwide at hardly any cost, simply by pressing a button. In such an environment the rules on data protection should be more expressly synchronised with the right to freedom of expression.

I have made here a distinction between personal data contained in – or intended for – traditional registers and such data contained in text which has not been structured in order to facilitate retrieval of personal data. I realise that such a distinction can be criticised for not being distinctive or realistic. Today, text can also easily be searched through or organised in order to retrieve personal data. Sweden's experience, not least, of trying to apply the 1973 Data Act, which was based on a similar concept of personal data register, to the technological developments of the 1990s shows the difficulties involved. I nevertheless think that the distinction is valid even

today. There is, regarding data protection aspects, a fundamental difference between the situation where the controller of the file focuses on personal data and its easy retrieval and the situation where focus of attention is on the text, whether or not it contains personal data. The data protection principles, and certainly the EC Data Protection Directive, already contain several vague concepts which we can live with. And I think that the distinction outlined between a register and text would be as clear and useable as many of the existing concepts. I would, however, like to make clear that the situation where someone in fact is using the text to search for and compile information about an individual should be treated according to the rules applicable to processing of personal data in registers.

For the reasons stated, I believe that we need a different approach to data protection as regards the handling by automatic processing of text, which has not been structured in order to facilitate retrieval of personal data. What we need is a system that affords effective protection for the vital interests of the data subjects' right to respect for private and family life and at the same time is easier to understand and handle on an everyday basis. I think that a new system of data protection should concentrate on preventing abuse of personal data rather than on regulating every step in the processing of such data. As I see it, there should be a shift in focus from the handling of every piece of personal information to the ultimate goal, preventing abuse. I would like to give some examples of what I mean.

3 An abuse centred approach to handling of text

First, I would like to make clear that I think that the data subject's right of access to his or her data is fundamental also when it comes to personal data contained in text. This right enables the data subject to control, at his or her discretion, what data are used and to make objections. One problem with the right of access, especially concerning personal data contained in text, is that the controller of the file could have difficulties finding all personal data about an individual contained in text. The right of access must not lead to a situation where controllers design tools, which they otherwise do not need, to retrieve personal data in text. It should therefore be made clear that, in response to an access request, the controller is obliged to use only existing tools and make only reasonable efforts to locate personal data, taking into account *inter alia* the information provided by the data subject. The data subject's right of access must also be balanced against the rights and interests of other data subjects and of the controller. One piece of text can contain personal data about more than one individual, and the controller should not be obliged to disclose data about other individuals than the one requesting subject access. In certain situations the controller's interest in keeping the data secret outweighs the data subject's interest in having access to his or her data. This can be the case concerning for example text containing communications between the controller and his or her solicitor in connection with a law suit against the data subject.

I think it is fruitful to distinguish between two different situations: The internal handling of text by the controller of the file and the controller's intentional or unintentional dissemination of the text to external recipients, including publication of text as well as disclosure of text to a limited number of recipients.

The internal handling by the controller of the file of text containing personal data, which has not been structured in order to facilitate retrieval of personal data, is seldom problematic. It is principally two situations that need attention.

Firstly, a controller should not be allowed to collect an unreasonably large amount of text about an individual without a legitimate reason. Even if the controller does not use the collected data in any way, most people would probably think of such an accumulation of personal data as an invasion of privacy.

The second situation is when the controller is using text containing personal data to base a decision which significantly affects the data subject. In this situation the data subject could use his or her right of access to the data to check what personal data have been used as a basis for the decision. What could be required is a right for the data subject to have the decision re-evaluated by the controller in the light of any objections raised by the data subject. An alternative, or supplementary, strategy would be to require that the controller beforehand communicate to the data subject all data on which he or she intended to base a decision.

The more problematic situation is when the controller disseminates or discloses text containing personal data. Most countries with data protection legislation probably already have legal protection against defamation, slander and libel. What is necessary apart from that is a general protection against the dissemination or disclosure of text containing personal data in a way that harms the data subject. The dissemination of text to a wider audience (publication) should, however, be allowed, if the controller was obliged to give an opinion or if the dissemination is otherwise justifiable having regard to the public interest. Harmful disclosure of text to one person or a limited number of persons should in addition be allowed insofar as the disclosure is justifiable, having regard to the legitimate interests of a natural or legal person, including the controller.