Information Technology and Legal Education: Towards 2000

9th & 10th April 1992
Sponsored by
Context Ltd; Linklaters & Paines; Needham & James

European Data Protection

Peter Blume

Institute of Legal Science, University of Copenhagen

Keywords: Data protection - human rights - the EEC single market - computer law teaching.

Abstract: The starting point is that the legal regulation of access to and use of personal data has gained increasing importance on an international level. After a brief historic account of data protection the general goals for such rules are discussed. In particular the distinction between different types of data is analyzed. The question of whether there should be different rules for the public and the private sector is considered. With this background the conflicting interests of data users and data subjects are discussed and the necessity for balanced rules is emphasized. After these general remarks selected rules from the EEC draft directive on protection of personal data are discussed. Finally the inclusion of data protection in the curriculum of law schools is highlighted among other things as a way of promoting a mutual understanding of legal protection of citizens across the European borders.

1. Introduction

Data protection has in recent years become a field of major interest for computer law in Europe. More and more European states have enacted statutes and the European Community is expected in 1992 to issue a directive which sets up common standards for the level of data protection in the member countries aiming to make it legally possible for personal data to flow freely within the community. While previously it was the Council of Europe that was the leading international organization for regulation of data protection on the basis of the data convention no.108/1981 it is now likely that the most important rules will derive from the EEC. As rules on data protection in many ways are closely linked to the general legal culture communicated by the legal system and as many rules can be viewed as the adaption of human rights in the modern information society this part of computer law is in particular relevant for teaching and research within the curriculum of law schools as it provides the possibility for promoting a mutual understanding across the traditional European borders.

The increasing importance of data protection makes it necessary to consider which goals these rules should promote and how the conflicting interests in the future ought to be balanced. In this

connection it is appropriate to take a closer look at the proposed EEC-directive and especially at those rules and principles that promote harmonization and development of a European standard that probably in the coming years will have a global impact. With such an background it is possible to consider how data protection issues can be integrated in the law curriculum and in this respect what level of knowledge future lawyers should have. These are the main questions discussed in the following.

2. Scope and goals

The emergence of data protection laws, starting in Hessen 1970 and Sweden 1973, was closely linked to use of computer technology as a tool for collecting and distributing personal data. The main assumption behind the different rules is that computer technology means that much more data will be gathered and used in a very effective way leading to a situation where sensitive data is diffused in an uncontrollable way throughout society. Such a situation creates major risks for invasions of privacy and misuse of personal data. The main purpose of data protection rules is that the potential possibilities of modern technology are limited. This is in itself important to take into account when considering the regulation as a whole. In general the legislation cannot be criticized for restricting computer technology as this is its primary purpose.

Since the first laws many technological developments have occurred leading to a change in the general environment for the legal rules. For the understanding of the problems discussed below it is appropriate to highlight these developments here. First of all the material has become smaller and cheaper. In particular the personal computer is the result of this development. This means that many more people and enterprises have computers and thereby the means for production of files. The number of users has grown very fast. The second major development has been new methods of storage that makes it difficult to locate data. This is in particular networks which among other things mean that it has become problematic to use the file as the main concept in the drafting of legal rules (see below). Today computer technology in its different forms has become a natural part of society. It is no longer a strange new technology that just for this reason makes people fearful. We know much more about the technology and how it can be used. It is with this background that the goals of the legislation and the dangers inherent in these goals must be considered.

2.1. Human rights

When determining the goals of data protection a reasonable starting point can be the human rights involved. Most important in this respect is the right to privacy as determined in the European Convention on Human Rights article 8. As is well known there exists an immense literature concerning the meaning of privacy dating back long before the convention. Several formulas such as "the right to be let alone" and "the right of self-determination to information about yourself" has been discussed and advocated. It is also well known that the need for privacy differs from society to society and is dependent upon social, moral and political norms that are constantly changing. It is accordingly important to note that from the concept of privacy certain pieces of information concerning a person must be his own, protected by legislation, but the concept cannot in any exact way tell us how data protection rules should be drafted. Privacy is not a creed that once and for all determines the contents of data protection as it only indicates that such rules must exist to ensure a satisfactory level of privacy.

Another relevant human right for data protection is the right of communication as outlined in the convention's article 10. Normally this right is referred to as the right to free speech and it is considered just as fundamental as the right to privacy.

It is well-known that in certain situations a contradiction exists between these two rights. When e.g.

certain utterances under criminal law are determined as libel this favors privacy but restricts free speech. The legal system has to find a very delicate balance between these two rights and this is also the case within the field of data protection. This fundamental problem must be taken into account when the goals of data protection are being determined.

2.2. The general goals

The primary goal is that sensitive personal data should only be filed when societal legitimate interests makes such filing necessary and filed data should only be diffused to others for the same reasons. As outlined below, this is not descriptive of current rules, but is my starting point for how workable rules should be drafted. Crucial problems in this respect are what should be understood as sensitive data, whether sensitivity is relative, i.e. differs as to which purpose filing and distribution aims at, who is responsible for it and whether the assessment should be influenced by the technology used, i.e. does computerization make special rules necessary.

Before these questions are addressed it should be noted that the rules, as discussed in the next section, must strike a balance between the interests of data users and data subjects. This can modify the practical consequences of the goals formulated in this section.

It is not difficult to agree upon the idea that sensitive data must be protected but it is not easy to reach a common standard for which data are sensitive. There are in this respect two extremes. One that all personal data can be sensitive, the other that only very few kinds of data are sensitive meaning that much personal data should be free to use. As a start it must be recognized that this is a political problem. Not least in especially first generation data protection statutes there was a clear tendency to make rules for the handling of all personal data but it was also recognized that some types of data are in particular sensitive and for this reason had to be more strongly protected. This line of thought is also evident in the EEC draft directive although its general tendency is to treat all data as potentially sensitive. As the information society has developed the amount of data has grown to dimensions that makes it necessary to take a new look at which data should be protected. It does not seem realistic to give all data the same protection today.

2.4. Kinds of data.

With this background it should be assumed that data can be divided into 3 categories. The first is data of a truly sensitive nature which must be given maximum protection. This is information concerning e.g. criminal offenses, sexual inclinations, political opinions, health. Such data should only be allowed to be filed when very strict conditions outlined in statutory form have been fulfilled. It is not reasonable to impose total prohibitions but a starting point must be that in particular in the private sector it is only very seldom legitimate to file such information. If this category of data is clearly defined it will be possible to make such strict rules work in practice.

The second category is data that although not sensitive should be treated as confidential, i.e. not freely known by anybody. It can be quite difficult to specify which data should be placed in this category but examples can be information on economic matters, tax affairs, and, if such a system exists, the personal identity number. The conditions for filing such information should not be as severe as for sensitive information but they should make it clear that there must be a legitimate reason for filing and distributing such data.

The third category is trivial data, e.g. name, address, telephone number, which should not be regulated, meaning that it can freely be filed. It is accordingly assumed that such data in almost all situations does not belong to the private sphere meaning that knowledge of such data does not make it possible to infringe privacy. This assumption is not consistent with existing rules where e.g. the

Council of Europe Convention protects all types of data. In my opinion it is as a starting point necessary to exclude trivial data in order to achieve a practical data protection. This makes it possible to concentrate the rules around those data that truly need protection and at the same time makes it possible to develop rules that are acceptable for data users which is a precondition for these rules to function in practice (see below). The conclusion up till now is accordingly that data protection should be limited to sensitive and confidential data.

2.5. Purpose of filing.

Another major problem is whether the purpose for filing information should determine the contents of the rules. Many different purposes form the background for filing and use of personal data. It is not possible within this paper to discuss all these and this is not really necessary as the important problem is whether the purpose in itself should be a parameter for the contents of data protection rules. In this respect it is sufficient to mention certain purposes that traditionally have been the subject of special consideration. Examples of such purposes are direct marketing, where trivial data are normally used, files for the purpose of warning against doing business with certain persons, credit information files, recording of data for control performed by public authorities. It is easy to see that such purposes can make it reasonable to have special rules. These should not be aimed at certain forms of data but determine how personal data can be used for each of these purposes which, when seen from the point of view of privacy, can pose a danger. This might also imply that trivial data can be involved but this should only be the case when the purpose clearly makes this necessary and should accordingly be treated as an exception.

In this connection it is in particular direct marketing that can be problematic. From the discussion above it is clear that sensitive or confidential information should not be used for this purpose but what about trivial data. In some statutes, including the Danish, there are provisions which limit the use of such data for this purpose. This is due to the belief that direct marketing for many people is a disturbance in their daily life and also due to the common interest in consumer protection. In my opinion this question should not be seen as a data protection issue and the legal rules should not be based upon considerations to privacy. This point is made to emphasize that even though trivial data are not covered by data protection there can be other legal rules that apply to such data.

In general the purpose for filing can be taken into account but it must clearly favor a certain regulation. It seems better to develop the rules around such purposes than to treat all data in the same way.

2.6. The data user

Another question is whether it is important who is responsible for filing the data. The main problem is whether there should be a difference between the private and the public sector. Some countries have only made rules for one of the sectors, others make the same rules applicable to both sectors. Denmark has separate acts for each sector. It should be taken into account whether the data user is a private firm or a public authority as the legitimacy of filing is influenced. Due to the tasks that public authorities are obliged by law to perform in many cases they have a legitimate interest in filing information which it should not be permissible to file in the private sector. It should be recognized that the possibilities of ensuring compliance with the rules are different in the two sectors and that the probability of the rules being respected is higher in the public than in the private sector. Although many rules can be similar these differences makes it reasonable to have separate rules.

In certain other situations it can also be taken into consideration who the data user is. In the private sector it seems reasonable to make special provisions for associations. There are constitutional reasons for protecting the freedom of associations and accordingly the relationship between an

association and its members should be excluded from the scope of data protection. Due to the major consequences for citizens that registration by credit rating agencies can have, these must be regulated by special rules that in particular ensure correct and fair filing of data. All in all it can be concluded that the goals of data protection must be adjusted in accordance with whom the data user is.

2.7. File or data

In the previous discussion emphasis has been laid more upon the concept of data than on file. This is in contrast with many European statutes where the objectofregulation is the file rather than the data. The choice of approach is important when it is to be considered what computerization means. This problem should be addressed from the perspective of the data subjects. Does it for the citizen have any relevance whether his data is filed ona computer or manually? The question can also be rephrased in such a way that it asks whether a data user should be allowed to file and distribute more data in manual than in computerized form.

As a starting point it seems clear that for the protection of privacy there should be no difference and that it is accordingly most reasonable to use data as the main object of regulation. The approach in the EEC draft directive that includes both manual and computerized files must therefore be preferred for the Council of Europe Convention that only covers computerized files. The fundamental rules as to when information can be filed and when it can be distributed should be the same. This will provide a more consistent regulation.

This however does not mean that it can be totally neglected that a computer is used. This is mainly relevant with respect to the question of security where it is clear that special guidelines are necessary to prevent unauthorized access to data. Also with respect to the possibility of matching, computerized data is special and rules are necessary. With these exceptions there does not seem to be a need for special rules.

This conclusion fits well to the fact that use of computers has become so widespread but it must be emphasized that the dangers of computing should not be neglected. To a certain extent mutual rules can increase the use of computers as there no longer will be a possibility of circumventing data protection by using manual means of storage. It must be added that inclusion of manually filed data does not mean that data protection falls without the domain of computer law as computerized data more and more will dominate the field.

2.8. conclusion

Concluding this section the following can be stated about the goals of data protection. The main goal is to ensure privacy with respect to such personal data that can be characterized as either sensitive or confidential. This goal is to be achieved through statutory rules that state clear conditions for when such data can be filed and distributed taking into account the purpose and the identity of the data user. The goal refers to data in any form and it aims at protecting citizens againstmisuse of data and at providing possibilities of individual control as to how data is used. Furthermore it is concluded that computerization only marginally influences the content of the rules as fulfillment of the goal must be independent of which technology the data user implements. Accordingly only special rules regarding the dangerous aspects of computing are needed.

3. Data user V. Data subject

With this background the balancing of different interests can be discussed. It is a common assumption that conflicting interests exists between data users and data subjects. Current data protection statutes are attempts to balance these interests. With the development of the information

society within a new age of data protection it is worth while reconsidering where the point of balance should be placed. As a starting point it is appropriate to consider what the interests of the two groups are and whether it is correct that these interests are conflicting.

First the situation seen from the perspective of the data user. At first glance it is in his interest to be able to file the maximum amount of data and to use this data freely. For some data users this is probably a fair description and it is clear that computerization has made excessive data collections possible. It is however not all users who have a uncritical attitude to which data they process and at the same time it should be taken into account that data filing can be expensive. There are certain restraints on data users but it is in many cases reasonable to assume, also when the value of information is taken into consideration, that many data users, both private and public, will collect more data than should be permitted.

The important assumption in this respect is that more data than necessary for the purpose of the data user is collected. If this is correct data protection rules can be seen as a guiding help for data users preventing these from being tempted by the possibilities of modern information technology. Data protection rules should from this perspective not be seen as rules against data users but more as common standards for the excecution of the different purposes that imply use of personal data. In the private sector the rules can be viewed as regulations on competition aiming at giving all firms within a certain field the same conditions with respect to data. From this perspective data protection is in the common interest of data users. This is not the case in the public sector where the rules in a more classic way aim at setting boundaries between the state and the citizens. Economically the rules can contribute to the reduction of public spending and limitation of bureaucracy. Also in this sector data protection is not a one-sided weapon against data users.

Secondly the interests of data subjects, i.e. the citizens. A basic starting point is that citizens in many relationships are interested in their data being used but need protection against it being misused. Absolute privacy is not in the interest of data subjects. This means that to a certain degree there are mutual interests between data users and data subjects. This is the case both with respect to the private and the public sector. It is therefore dependent on the individual purposes to which degree citizens are interested in data usage. To ensure that misuse does not take place data subjects are interested in clear rules defining when in particular sensitive and confidential data can be filed and distributed. More than this they are interested in an open and transparent practice where there are good possibilities of knowing when personal data is used and a possibility of controlling the correctness of data. In many ways the essential demand is that data subjects are well informed.

The difficult question in connection with drafting precise rules is to balance the data users interest in filing large amounts of data against the data subjects interest in more limited filing. The balance point must be fixed on the basis of general societal considerations taking their starting point in the purpose for filing and distribution.

A good example is credit information. Credit rating agencies want to file all kinds of data that can have any bearing on the creditworthiness of the individual citizen. This will include data of a sensitive nature. The individual data subject will not be interested in any filing at all because this means that he might not get credit. Society as a whole views credit rating as one of the tools for making market economy function. It is necessary to have an instrument enabling enterprises to decide whether credit is to be given. Accordingly it is clear that these agencies must be allowed to register certain data that makes credit evaluation possible. A balance point has to be set up. In the Danish act these agencies are not allowed to file sensitive data (section 9, subsection 2). Has a citizen been convicted of issuing false cheques this can be useful for evaluation of creditworthiness but from a general point of view such information should not be used in this respect. Such a rule is of course open for discussion but is a good example of balancing.

In general data protection must not only provide protection of privacy but also make it possible for

legitimate reasons to file and use personal data. In the drafting of the individual rules both interests must be taken into account so ensuring that legislation does not become one-sided. This approach makes it more likely that the rules will be respected in practice and thereby serve their purpose. Under a dynamic perspective there is a tendency to acknowledge the interests of data users especially in countries with long traditions of data protection. This in the long run leads to more workable rules. Such abalanced regulation in many ways presupposes a developed data ethics in society; a question discussed below in section 4.

Here it is sufficient to state that balance and ethics are necessary both in the private and the public sector and therefore are some of the keywords for assessment of actual rules.

4. The EEC draft directive

After these introductory remarks outlining a general basis for data protection in the 1990's it is appropriate to take a detailed look at those rules which in practice will set the agenda in the coming years, the forthcoming EEC-directive on the protection of persons with relation to personal data. This directive which will be the first supranational regulation is the most important document since the European Convention and the draft of July 1990 must accordingly be scrutinized very carefully.

First an overview of the basic features of the draft directive. Its general aim as stated in article 1 subsection 2 is to ensure that personal data can flow freely within the community as member states are not allowed to prohibit data flow for reasons of protection of privacy. The aim is thus to build a single information market with the understanding that also personal data is an important feature of a modern economy. To achieve this general purpose it is necessary that all member states provide an equivalent protection of personal data and it is this that the substantial rules of the directive aim at.

The directive covers both manual and electronic files with only a few special rules on computerized data. It covers both the public and private sector. Two categories of data users are not included. These are private persons' files for personal purposes and association's files on members (article 3) Those parts of the public sector that fall without the treaty of Rome are of course also not included.

In general the rules provide a very high level of protection and with respect to the conflicts between data users and data subjects it is the last mentioned whose interests have been in focus. To a certain extent this is understandable. Internationalization of data can from the citizens point of view be seen as a danger for privacy. It becomes even more uncertain where personal data is and what it is used for. This development can accordingly in itself lead to fear from citizens and mistrust towards data users. It is therefore reasonable to ensure a high level of protection.

Although this is the case the need for balancing still exists and the restrictive character of the individual rules should not be exaggerated. For this reason it is doubtful whether this draft is suitable in all respects as the legal basis for data protection in Europe.

As it is likely that many of the rules will differ from the draft in the final directive only a few of these will be discussed in the following. This will be done by highlighting certain themes of relevance for the general design of data protection rules.

4.1. Procedural rules

The first theme concerns the question of bureaucracy, i.e. the procedures necessary for establishment and use of files. This is quite a difficult problem as it is linked partly to the possibilities of public control with data users and partly to the level of information given to data subjects. At the same time very bureaucratic rules will lead to a negative image for data protection at the data user level which

is unfortunate because in the long run these rules depend on a voluntary co-operation from data users.

In the directive it is stated that public files from which data might be communicated shall be notified to the supervising authority (article 7). Also private files from which data that is not publically accessible is communicated shall be notified (article 11). When data from a public file is communicated to the private sector the data subject shall be informed or prior authorization from the supervising authority be obtained (article 6, subsection 3). The first time data is communicated or on line retrieval made possible in a private file the data subject shall be informed unless communication is required by law (article 9, subsection 1).

When assessing these rules it must be taken into account that they are directed towards both manual and electronic files and also that all kinds of personal data are included. Very extensive obligations are accordingly instituted. The rules make it necessary to have a large supervisory bureaucracy and it will mean that citizens will be showered with information. In my opinion these rules are an example of overkill and for this reason are counterproductive in the sense that they can easily produce a negative attitude towards data protection, not only from data users but also from data subjects. In this connection it must be taken into account that too much information can mean that data which is relevant under a privacy perspective will not be noticed by many citizens.

Generally for the development of European data protection culture it is important that the rules are given the right proportions and they should as indicated above concentrate on sensitive and confidential data. Only files containing such data should be reported and only with respect to communication of such data is it reasonable that citizens are informed. However it should be added that it is correct to focus on communication rather than filing. Communication implies more risks for privacy and well informed data subjects are necessary.

4.2. Rights of data subjects

A second general theme which has already been touched upon concerns the rights of data subjects, i.e. the possibilities for control of the use of personal information. This theme is given great consideration in the draft directive, where the rights are outlined mainly in articles 13 and 14. To a certain extent these rights are new in comparison with many of the existing data protection acts.

First of all in article 13 a right of information in connection with collection of data is given. The data subject must know for what reason data is collected and whether it is obligatory to answer questions. Information to citizens before data is filed is in many ways important as to a certain extent it makes prior control of filed data possible. It is of course limited to situations where data is collected from the data subject but together with the above mentioned rules on communication it ensures a quite high level of information. The right to information on collection is reasonable and does not impose practical difficulties upon data users.

In article 14 several other rights are given. Among these is the right to have wrong data corrected and the classic right of access. It is through access that the data subject can control his own data and although this right traditionally is not very much used it is important. In particular it can be noticed that access cannot be excluded in the private sector which in many ways is reasonable as the legitimacy of possessing data in this sector must be dependent on an open relationship with citizens.

In article 14 no 6 a right to be deleted from files used for market research or advertising purposes is given. This is an interesting rule in connection with the above stated remarks concerning trivial data. It is here assumed that e.g. marketing in itself can be conceived by some citizens as infringement of privacy and for this reason they shall have the right not to be included in such files. The attitude of citizens towards direct marketing is very different and seen from an individual point of view this is a

reasonable rule. On the other hand it is not a necessary part of data protection and for this reason is an example of the sometime too broad scope this legal domain is given.

All in all the rights given to data subjects although extensive are not of a nature that undermines the balance of data protection and these rights are also in many ways necessary for the general acceptance of data usage. They are important because they indicate the standard for an essential part of citizens' rights in modern Europe.

4.3. Research purposes.

A special problem-area is the use of personal data made in connection with research. Use of data for research purposes is not explicitly dealt with in the draft directive but one rule of great importance should be mentioned also because it demonstrates the many different considerations connected to data protection rules.

This is article 16 subsection 1 e in which it is stated that data must be kept "no longer than is necessary for the purpose for which the data are stored". This is in many ways a well-known rule that aims at preventing storage of unnecessary or obsolete data, but the problem is that there are no exceptions to this rule. This means that there is no possibility of placing data in archives etc. meaning that research within many different scientific fields in the future will be very restricted and where the end result very easily can be that in the future we will know more about the society of 1902 than of that of 1992. This is accordingly an example of the complexity of data protection where it is fairly clear that transfer of data to archives where it can be secured satisfactorily does not pose any threat to privacy.

This special problem is also metioned because it represents a question in which researchers across borders have mutual interests and co-ordinated action can be well founded. Reasonable considerations to scientific research should be a small, but nevertheless important, element in European data protection culture.

4.4. Data protection ethics

Article 20 obliges member states to "encourage the business circles concerned to participate in drawing up European codes of conduct or professional ethics in respect of certain sectors on the basis of the principles set forth in this directive". The variation of topics covered by data protection and the character of regulation means that it is very difficult in statutory form to determine all aspects. At the same time the rules are dependent on a certain measure of understanding from data users. Such legal rules are well suited to be combined with ethical standards. Article 20 is accordingly important although it could have been worded more strongly and also should have included the public sector. It is clear that many sectors and br types of data users have special problems and also traditions which can be covered by an ethical standard. As such standards will be drafted by data users it is likely that they will be respected and can become a very effective instrument of data protection.

It seems important that drafts of such standards are discussed openly and that representatives of data subject interests are active in such debates although it is hardly possible to construct something like "agreed documents". Also academics should be active in this respect. When the standards have been made they should be published so that data subjects have a possibility of knowing them.

When the general aim of the directive is taken into account it is also stated in article 20 as important that the standards are European and not merely national. Standards will also be an adequate instrument for the promotion of cross-border understanding. It can be concluded that drafting of

these standards is an important part of the agenda for the 90's.

4.5. Control and real harmonization

An EEC directive implemented in national legislation is not in itself a sufficient guarantee for mutual European data protection. To achieve this goal it is not sufficient to have the European Court to decide concrete cases of which there will probably not be many. It is necessary to have administrative authorities on a European level to control the implementation of the rules and to co-ordinate the adjustment of the rules made necessary by technological developments etc.

The draft directive is aware of these questions and institutes different organs for control (articles 27-30). Although the proposed structure is quite bureaucratic it is fundamental that such organs are set up. In particular it is important, as also indicated in article 28 subsection 2, that it is made possible to compare practice in the different countries with the purpose of harmonizing this within the framework of the directive.

In this respect it is necessary to consider who should be placed on these committees. In the directive these are representatives of national governments and supervisory authorities. It would however also be relevant to include independent observers of data protection, experts, who in many ways have the best possibilities of ensuring a meaningful balanced regulation in practice. Academics from the different European countries should be active on the European level and have formalized channels to communicate their opinions.

4.6. Conclusion

All in all the directive will when implemented provide the basis for development of a real European data protection culture which will also have global implications. The directive will be a major vehicle for harmonization and will on many different levels favor co-operation across borders thus placing data protection strongly on the agenda for computer law in the 90's. European computer law will have one more common subject that can be taught and researched in many countries.

5. Teaching data protection law

Data protection is a main feature in the legal regulation in the information society and with the EEC directive common standards for this legal field will emerge in the European countries. Furthermore when it is taken into account that these rules are gaining increased importance in the legal system at the same time as they concern fundamental questions for citizens and thereby are part of the legal culture of society it seems clear that data protection should have a place in the curriculum of law schools. This will enable a higher mutual understanding between lawyers in the different European countries.

In Denmark, as I suspect is the case in most countries, faculty boards are rather conservative and it is difficult to get new subjects introduced especially in the compulsory parts of the curriculum. Although a strong case can be made for data protection law both from a practical and theoretical point of view it is necessary to consider how such an introduction can be achieved.

The most ambitious solution is that data protection law becomes an individual topic with its own exams etc. This does not seem realistic in the near future. There are 3 other possibilities which can also be combined.

First the subject can be that of privacy, including not only data protection but also e.g. traditional

criminal law and press law. Such a subject could be useful for the education of lawyers with high awareness of legal rights for citizens. Another possibility is that data protection occupies a major place in computer law or as we often prefer to name the subject in the Nordic countries, legal informatics. To a certain extent this is feasible, but the inclusion of manually processed data will pose some problems. Thirdly data protection issues can be integrated into the traditional subjects such as administrative law, criminal law and commercial law. This model has the well-known risk that these new questions in practice are not given sufficient attention. Although it is important that the old subjects are renewed and adjusted to the realities of the information society it is not fortunate if this becomes the sole model. Personally I prefer a combination of these three models and would recommend that they are applied at the same time.

The European perspective is important in the actual teaching. Data protection should not be taught as a national subject, but as an international. This dimension should not only include international documents, but also on a comparative basis the appropriate rules of other national acts. This subject is accordingly also well suited for courses within the Erasmus program. If priority is given to the international dimension, data protection law will become a subject that can promote a mutual understanding of the legal protection of citizens in the European information society. This must be a major goal for the development of legal education in the coming years.

Author
Peter Blume
Institute of Legal Science, Section B,
University of Copenhagen
Studiestrade 6,
1455 Copenhagen K,
Denmark