For many years, Italy and Greece have lagged behind other European Union Member States in terms of adopting a comprehensive data protection law. Their lack of such a law has provided one of the reasons for adopting the EU Data Protection Directive. Now there are signs of change. Greece, under a new prime minister, has prepared a new draft law which reflects the EU Directive’s requirements. Italy, only narrowly, failed to adopt a bill at the end of last year. Now, Italy’s new government has given the revived bill priority status to speed its passage through the legislature (p.2) and it is expected to be adopted later this year.

There are signs of the Member States now tackling with urgency the challenge of transposing the EU Data Protection Directive into national law. Sweden and Spain have officially designated their Data Protection Authorities as their official supervisory bodies. The Netherlands is close to a draft law. Belgium’s Conseil d’Etat cited the EU Directive when giving its advice on the draft royal decree on exemptions from registration, published in Le Moniteur Belge on 15th March. Germany’s Federal Data Protection Commissioner has submitted a paper to the Interior Minister. Denmark has established a committee, chaired by the former director of the Register syrup, which also includes the current director and the leading academic expert. The UK’s Data Protection Registrar has published a detailed paper inviting all interested parties to join the debate (p. 16).

Of course, domestic agendas remain. Public spending cuts have encouraged some fundamental thinking on the resources which can be devoted to funding the work of Data Protection Authorities. The Director General of Sweden’s Data Inspection Board discusses the limits of her powers in an increasingly computerised society (p. 7).

The UK’s Home Office published, on 19th June, its white paper on access to criminal records for employment and related purposes. We will discuss the policy implications for employers, the police and the individual in our next issue.
Italy’s new government gives priority to data protection bill

Italy remains the only European Union Member State, together with Greece, where a comprehensive data protection law has not yet been enacted. The Privacy Laws & Business Newsletter has been reporting on successive bills since 1987. However, this month, the new government submitted data protection bills to the Chamber of Deputies and Judge Giovanni Butarelli, the principal author of the bills, based at Italy’s Ministry of Justice, reports that the new government has made use of the “priority route” to facilitate adoption of the draft legislation. Here he explains the background to the bill and then summarizes the main features.

In 1989, Italy’s Parliament authorized the ratification of the Council of Europe Convention no. 108. The instrument of ratification has not yet been deposited. No general law in Italy governs data protection. Instead, special provisions apply which are found in different laws.

In November 1993, Italy’s Chamber of Deputies approved, almost unanimously, a data protection bill (no. 1670/S). However, in February 1994, it came to a halt in the Senate owing to heavy pressure exerted by a number of organisations in the private sector which opposed provisions, especially the protection of data relating to legal persons.

Following national political elections in March 1994, the Ministry of Justice considered a few modifications aimed at ensuring undiminished protection of personal data with less red tape and general costs for data controllers, for example:
• a few cases of exemption and simplification regarding notification
• the number of provisions applying to data on legal persons was reduced
• a few periods of time laid down in the transitional provisions were extended
• the “principle of intent” was given greater weight regarding a few criminal offences.

In January 1995, the Italian government approved a new bill (1901/C) whose framework was largely similar to the previous one, although introducing modifications in accordance with the text of then current version version of the EU Data Protection Draft Directive. The bill aimed to implement the basic principles in the Council of Europe Convention and took into consideration the EU Directive, except for a few issues, such as applicable national law and transfers of data to third countries which will be addressed at a later stage.

Following a lively debate of over 10 months duration, the bill was approved without major amendments in November 1995 after having been split into two separate items (no. 2296/S and no. 2343/S). Dissolution of Parliament in January 1996 prevented the bills from being passed at this stage.

However, on 7th June this year, the Government which resulted from the general elections of 21st April, again submitted the bills to the Chamber of Deputies without any amendments, in order to make use of the “priority route” established by parliamentary regulations. Obviously, changes may still be made to the texts. The new government has stated that it intends to deposit the instrument of ratification of Council of Europe convention no. 108 immediately the bills are adopted into law.

Public opinion pushes bill forward

The temporary exclusion of Italy from the Schengen agreement, owing to the absence of a data protection law, caused an uproar in the media and public opinion. For the first time since there was an attempt to adopt a data protection bill in 1975, the new government went beyond a formal commitment and undertook to rapidly approve the current data protection bill. The approach favoured by the law’s opponents, to approve a data protection bill relating only to the Schengen Information System, was considered not practical. Instead, the government considered that a comprehensive law was necessary to allow ratification of Convention no. 108.

Reactions to the bill were mixed. The bill was judged favourably by all branches of the public administration. Conversely, despite the many amendments meeting the requirements of the private sector, it was received with greater and more spirited opposition by publishers, computer equipment companies, insurance companies, small and medium-sized companies which fuelled a
lively campaign against its approval in the press and through reports submitted to Parliament.

**Timetable**

It is expected that the bill will be finally approved by September 1996 and enter into force in January 1997. By the third week of June, 23 of the bill’s 45 articles had been approved.

The long period of discussion in Parliament is due to the painstaking paragraph by paragraph analysis by the parliamentary review committee and a lively debate caused by the mass media’s request for exemption the provisions of this law which many parliamentary groups considered out of all proportion to their perceived problems with the bill.

The competent parliamentary committee strengthened the safeguards provided for in the government’s bill, for example, by establishing the same rules for automated and manual data. The committee has not, so far, considered any amendments conflicting either with the principles of the Council of Europe Convention no. 108 or with the principles or with the guidelines proposed by Italy’s private sector.

Probably, for the first time in the history of the Italian legal system, the bill expressly mentions the Council of Europe’s individual recommendations in the field of data protection, including R (95) 4 on telecommunications. The bill provides for the issuing of delegated legislation in which the general data protection principles set out in the new law will be implemented through specific regulations governing the individual areas which are covered by the Council of Europe recommendations. These regulations must follow guidelines established by the new law.

**Progress on other data protection initiatives**

Italy has ratified EU Directive 388 on access and competition in the field of telecommunications and introduced a clause which specifies that there will be no prejudice to the implementation of any provisions on data protection approved in the future.

The most widely debated data protection issue concerns the relationship between data protection and the new telecommunications media; and the way in which future legal provisions governing the transfer of data to third countries should be applied to Internet connections.

It is widely expected that a law will be adopted which would include:

- establishing the responsibilities of service providers and users
- whether anonymous access to bulletin board systems should be permitted, and
- whether encryption systems may be used.
Italy’s Data Protection Bill’s main features

Italy’s Constitution includes provisions relating to data protection. Such provisions define the ‘level’ of the balance of interests involved - as seen also in the laws concerning personality rights and in those governing economic activities. The laws concerning economic activities, according to jurisprudence, cannot be in conflict with the principles of personal freedom and human dignity. Moreover, there are several ‘special’ laws (Workers’ Statute, AIDS laws, right of access to public documents) which the bill leaves intact.

Scope of the Bill: The new data protection law will not immediately apply to police data files (which are governed by Law no. 121 of 1981), to intelligence agencies, to justice or to matters under State secrecy - except as related to the principles of data security, quality of data, automated profiles and control by the supervisory authority. Still, the new data protection law will immediately apply to these sectors with regard to those articles allowing immediate ratification of the Strasbourg Convention and the Schengen Agreement. It will be determined, through delegated legislation, whether, and the extent to which, some principles may be applied to the processing of the above data.

Manual data: Manual data falls within the scope of the bill. The preceding Government has proposed that manual data should be governed by this law only if it was (or was expected to be) included in data files. The preceding Parliament held that they should be protected in any case.

Public and private sector: This distinction is related above all to the procedures for obtaining the data subject’s consent. Consent is required only in the private sector, as an alternative to the requirements that are set out in the EU directive.

Information to the data subject: It is to be provided only at the moment of data collection (except for cases of right of access). Parliament can be expected to introduce amendments which entail further obligations in this area, as is provided for under article 11 of the EU Data Protection Directive (95/46/EC).

Data subject’s consent: Consent is to be given in writing only for sensitive data. In other cases, express consent (orally or in writing) must be given freely and in a specified form.

Notification: To facilitate control by the supervisory authority and exercise access rights:
- a simple notification is available covering a wide range of personal data classes
- a similar notification applies to data transfer to third countries
- a special authorization is required for the processing of sensitive data.

Security: This principle has been assigned a high level of priority, with effects in the fields of civil and criminal legislation. Specific decrees will set out more detailed rules. Special safeguards are required for appointing a data processor and a processor must comply with them.

Legal persons and deceased persons: Data relating to legal persons falls within the scope of the bill as well as those concerning various other bodies. The processing of such data is not governed by the rules applying to the transfer of data to third countries and to the right of access. The rights concerning deceased persons may be exercised by those who have a justified interest.

Supervisory authority: The powers conferred on the independent supervisory authority are wide-ranging and include:
- keeping of the registry of processings,
- powers of direct access, and
- control.

Any data subject may apply to the supervisory authority either through a simple claim or by formally lodging a complaint which institutes a legal proceeding. The final decision rendered by the authority at the end of this proceeding is to be complied with under sanction of a criminal penalty. Such a decision may be appealed against by legal means. The data subject may also decide to apply directly to the judicial authorities.

Other features: The bill also includes: the concept of anonymous data, an equal discipline for temporary processing, rules concerning codes of conduct, transitional provisions, administrative and criminal punishments, regulations applying to research and statistics, provisions governing transfer of data to third countries.
Ontario defines privacy protection principles for voice mail systems

Information and Privacy Commissioner for Ontario, Tom Wright, issued, last October, a set of privacy protection guidelines aimed at users of voice mail systems. This is a third in a series of extremely useful papers produced by the Commissioner’s Office to help organisations in both public and private sectors deal with privacy issues, related to technology in the workplace, arising from the widely used facilities and technologies - facsimile transmission, e-mail and voice mail systems. The Privacy Laws & Business Newsletter has already reported on guidelines for fax transmissions and e-mail systems (PL&B, Feb 1995, p.4, Dec 1994, p.8). Both private and public sector organisations should find the voice mail principles useful in their development and implementation of corporate voice mail policies.

The widespread use of voice mail and its popularity continues to expand on a daily basis. Many advantages have been recognised by its users; it facilitates communications, improves customer service, reduces time spent on hold, returning calls or talking on the phone. It can even enhance privacy since personal messages are communicated directly to the user, rather than through someone taking a message.

However, the voice mail system also has a negative side. Insecure systems or improper set-up and implementation can result in privacy breaches, as well as poor customer service. Voice mail security becomes even more critical with developments in technology and computer systems being increasingly integrated with telephone systems. These integrated systems can provide voice mail, e-mail, fax on demand, interactive voice response and other technologies at the desktop. The greater the number of connections, the greater the vulnerability of all those technologies to unauthorised access. That is where a corporate policy on privacy issues involved in these new technologies becomes essential.

Voice mail raises potential privacy concerns for senders, recipients and individuals who are the subject of voice mail messages.

The principles developed by the Information and Privacy Commissioner are not meant to be a standard set of guidelines applicable to all organisations. Due to different varieties and uses of voice mail systems, the guidelines are more of a framework for the development and implementation of an organisation’s own privacy protection policies for the use of voice mail. They may need to be supplemented by examples specific to an organisation in order to increase employees’ understanding of the principles.

The principles
1. The privacy of voice mail users should be respected and protected.

Voice mail should be considered a private communication between the sender and recipient. However, due to the inherent characteristics of most voice mail systems, it is not possible to guarantee complete privacy. It is up to organisations to ensure that the system is set up and operated to guarantee the best possible degree of privacy and security. Unless organisations strive to offer the highest degree of privacy, employees may be reluctant to use voice mail to its maximum potential, hence annulling all the advantages of using the system.

2. Employees should receive proper education and training regarding voice mail and the security/privacy issues surrounding its use.

The more users know about voice mail systems, the better able they will be to protect both their own privacy and that of others. Any training should make the employees understand the following:
• the voice mail process is not inherently private
• a message that has been sent or deleted may still exist
• voice mail systems can be broken into
• voice mail technology may work against privacy.

3. Each organisation should create an explicit policy which addresses the privacy of voice mail users.

A formal and clear policy on voice mail privacy creates employees’ expectations, helps to establish trust between employees and management, prevents litigation, wrongful termination law suits
and harmful publicity. Employees should be made aware of their rights and obligations under the policy and agree to adhere to it.

As a minimum, the policy should set out the following:
- approved uses of the voice mail system
- third party access to voice mail, including conditions and procedures for access
- consequences of violations of the voice mail policy.

4. Each organisation should make its voice mail policy known to employees and inform them of their rights and obligations regarding the confidentiality of messages on the system. All staff should be informed about their privacy rights and obligations regarding the use of voice mail in the workplace. By setting a clear policy and standard that everyone understands and agrees with, users will know what to expect regarding the confidentiality of messages on the system.

5. Voice mail systems should not be used for the purposes of collecting, using, retaining and disclosing personal information, without adequate safeguards to protect privacy.

Every coherent corporate voice mail policy has to recognise that in addition to protecting the privacy of voice mail users, individuals who are subjects of voice messages also require protection. Some features inherent to voice mail may contribute to breaches of fair information practices, such as the ease with which personal information can be intentionally or unintentionally sent/forwarded. The further personal information becomes from its original source, the more difficult it becomes to adhere to fair information practices.

Since recipients of personal information may be unaware of the original purpose for which the information was collected, they may inadvertently use or disclose it for an inconsistent purpose. For all these reasons, subscribers may wish to record greetings that discourage callers from leaving messages containing sensitive information.

6. Organisations should pursue technological methods of protecting voice mail privacy.

Organisations should conduct privacy impact assessments of proposed or existing systems to determine how and when privacy may be threatened and address vulnerabilities before problems occur. Security needs of each organisation will vary depending on the type of information that is communicated via voice mail and the system's level of integration with the office computer network. Therefore, a risk assessment should be conducted to determine the organisation's security needs and select a system with an appropriate level of security.

There are several technological ways in which the privacy/security of voice mail users and subjects can be enhanced. The security problems can be tackled and measures be implemented on three levels:
- by voice mail users
- by system administrators
- by automatic security features of the system.

7. Organisations should develop appropriate security procedures to protect voice messages.

Privacy protective policies and technological features will only be effective to the extent that they are accompanied by appropriate procedures to promote and maintain privacy, confidentiality and security.

New Fax Security Guidelines

The Office of the Information and Privacy Commissioner for Ontario has issued, for 1996, an updated set of Guidelines on Facsimile Transmission Security. First developed in 1989, and updated in 1990, the Guidelines have been revised once again as a result of the changes in fax and communications technology, increase in computing power, the use of networked systems, and the Internet, and the growing number of providers offering on-line services.

To obtain these documents, contact the Office of the Information and Privacy Commissioner/Ontario, 80 Bloor Street West, Suite 1700, Toronto, Ontario, Canada, M5S 2V1. Tel: +1 (416) 326 3333 Fax: +1 (416) 325 91955
What can Privacy Commissioners do? The limits of bureaucratic intervention

With limited resources and powers, it is clear that there are limits as to what Privacy Commissioners can achieve. The following report is an edited version of a presentation given by Anitha Bondestam, the Director General of Sweden’s Data Inspection Board, at a conference last month in Victoria, British Columbia, Canada. As Sweden adopted the first national data protection law in 1973, there is a long perspective to reflect on the role of a Privacy Commissioner in a changing society.

It sounds obvious that the limits of bureaucratic intervention are of at least three different kinds, limits prescribed by legislation, limits observed for political reasons, and limits observed voluntarily. Moreover, circumstances beyond control may impose yet a fourth set of limits. And finally, I have some ideas about how we might be able to perform our duties without being bureaucratic. I shall begin with the legislative limits.

1. Legislative limits

Sweden is a land of opportunities. In Sweden, there are virtually no limits to what the Privacy Commissioner can do under the law. The Data Act of 1973 - the oldest national Data Protection Act in the world - offers the Privacy Commissioner an almost unlimited right of bureaucratic intervention whenever personal data are “automatically processed,” be it in the public or private domain.

The Privacy Commissioner can issue directives, sanctioned by penalties, to private firms, organisations, local governments, governmental authorities, and private citizens. Each year we issue some 7,000 such directional rulings.

For inspection purposes, the Privacy Commissioner has the right of entry into any premises where personal data are processed, as well as access to all documents concerning such data processing.

Accordingly, Sweden should be the promised land for a Privacy Commissioner, that is, in theory. The real world, as so often happens, poses problems, among those not least the short time perspective of politicians.

2. Political limits

When the social climate changes, attitudes to the protection of privacy change as well. Today, the budget deficit is the overwhelming problem of the politicians. The problems of the Privacy Commissioner thereby are increasing, because protection of privacy does not come for free.

At the end of the 1980’s, there was no lack of funds in Sweden. One could afford to take a positive attitude to issues of privacy. The personal identification number (PIN), introduced in Sweden in the late 1940’s was looked at as an evil, a symbol of Big Brother, that had soon to be eliminated, at least in principle. For that reason, some rules were added to the Data Act in 1992, to limit the use of PINs.

Following the Canadian decision to reduce the use of PINs, the Swedish government in 1993 appointed a committee with the task of finding a cure for the excessive use of PINs. The committee recommended that PINs, now public, should be treated as secret. At the time the committee presented its recommendation, it was already 1994, and attitudes to new governmental expenditure had changed. Those public and private organisations invited to present opinions on the proposal delivered a devastating criticism, and the recommendation ended in the waste-basket.

Another example of a political limit concerns the pre-investigation police file.

A pre-investigation police file may comprise data on people who might have something to do with a crime but are not necessarily suspected of a particular crime. Somebody may have exited from a building where a well-known drug-pusher is resident, or has bought a car he “shouldn’t” be able to afford, or he has made a sizeable deposit in his bank. He does not know that he is on the police file, since there is no public access to those investigations. As late as in 1992, government turned down the idea of computerised pre-investigation files.

That was in 1992, however. Just two years later, the government changed a decision made by the Data Inspection Board, where the Board had refused permission to the Finance Police
Force, a service responsible for fighting money-laundering, to set up a pre-investigation file that might well contain data on the banking business of innocent individuals. This file gave no right for those registered to know that they were on the file. The economy and economic crimes had turned out to be more important than privacy.

And just recently, the former Director General of the Data Inspection Board, Mats Borjesson, commissioned by the government to study the issue, has presented a blue-print for a law both on a comprehensive pre-investigation file and a DNA file.

The climate has turned harsher. Just four years ago, government turned down a pre-investigation file planned to be kept in the hands of the police force. A couple of months ago, some banks applied for permission to set up their own pre-investigation file of “unusual” transactions. The Data Inspection Board of course turned down the idea, but the banks have appealed to the government. I dare say that just a couple of years ago, the very thought of a private criminal file would have been unthinkable.

A third example concerns cross-matching. By cross-matching, I mean obtaining data from one or more personal data file and transferring the data to a new file. Cross-matching falls under the provisions of the Data Protection Act and may only take place with the permission of the Data Inspection Board. The Data Inspection Board considers cross-matching acceptable, provided that the individuals the data refers to have been informed in advance that cross-matching will or may take place. In contrast, the Data Inspection Board does not accept the idea of issuing decisions on cross-matching after the event. Data collected for one purpose is not necessarily suitable for different purposes not envisaged from the outset.

So far, Sweden has undertaken a general census every five years. The purpose of this is to provide information to be used, among other things, for housing and road planning, statistics, and research. The procedure has included sending a questionnaire to all residents of Sweden.

A few months ago, government managed to push a bill through parliament, providing for the registration of all residents not just on their street address - that we have by old tradition - but by apartment number. The next step will come on the occasion of the next census, when the apartment register will form the base and other information will be entered by cross-matching from different data banks.

Accordingly, those registered will not be involved themselves. On the contrary, it will be the landlord and the next door neighbour, who will tell the authorities who he or she believes to be living next door. All this, believe it or not, is aimed at getting “good statistical data and good town planning.”

The Data Inspection Board has firmly opposed such a procedure that would be implemented behind the backs of the citizens. A corresponding procedure would make it possible to cross-match files currently used for the purpose of administering unemployment benefits, sickness allowances, or study grants, all for control purposes, but all without the knowledge of the individuals concerned.

3. Voluntary limits
The limitations are set not just by outside forces. As Privacy Commissioner, I also observe voluntary limits. A commissioner who wants to be taken seriously must use common sense when applying her authority.

Accordingly, we have set a goal for our operations at the Data Inspection Board: to strike the proper balance between the individual's interests in privacy and opposing legitimate public interests.

So the issue is where to put the limit between proper and improper data processing, for instance with respect to health data.

Recently, the Data Inspection Board turned down an application in which a team of doctors announced their plans to cross-match data on:

• a group of 250 tall females, who, in their teens had received medication to stop their excessive growth, with

• files on the incidence of cancer.

The women, now grown-up, would not be informed. The reason was the wish not to worry the women unnecessarily with the risks of cancer involved in their medication. But the application to the Data Inspection Board was public and became the subject of great media attention. Consequently, the damage had already been done.
application, the data subjects, of course, demanded detailed information.

I want to point out another area where development tends to get out of hand if we don't join hands to stop it, the commercialisation of official documents.

In most countries, public files exist, listing, for instance, all those holding drivers' licenses, all car-owners, and all land-owners. Public sector activities are expected to take place in the most cost efficient way possible, by saving expenditure or by contributing fees to the budget, preferably both. No wonder then that public authorities turn to the resource at hand that particularly enjoys increasing attractiveness in the market, and on which they have a monopoly: that is selling public sector information for commercial purposes. Where such policies have received explicit authorisation by the legislator, it does not seem appropriate for data protection authorities to question the political usefulness or the desirability of such activities.

Even against the present background of broad political consensus, or perhaps rather just because of this, data protection agencies should worry about these developments. They do affect the very principle of data protection. As described by Professor Herbert Burkert of Germany, three principles are jeopardised:

1) Commercialisation leads to a completely new type of data transfer.
2) Commercialisation strongly violates the principle of limitation of purpose.
3) Commercialisation endangers the principle of minimisation.

Swedish companies have great plans for using IT for commercial purposes. They feel that the Data Inspection Board unduly interferes with their plans for expansion, and that the rules laid down in the Data Act are an obstacle to free enterprise. Let me mention just one example.

The Swedish telephone administration was reorganised in corporate form - in preparation for privatisation - just two years ago. Its present corporate name is Telia. When Telia was formed, the corporation took over from the state monopoly administration its files containing details on all telephone subscribers in Sweden.

Recently, Telia applied for permission to set up and maintain a new file, containing not just the names and addresses of all the telephone subscribers in Sweden, that is, more than 60 percent of the population, but also personal data from the Motor Vehicle Register, the National Land Register, the Patent and Registration Office, and Statistics Sweden. The declared purpose of the file was to be able to provide "all the services and products for which there is market demand or will be in the future," for purposes such as direct mail advertising, market research, and tele-marketing. In other words, Telia wanted to create a gigantic population register for purely commercial purposes.

The Data Inspection Board made the following observation:

The purpose of Telia's subscribers register is to administer relations with its individual subscribers. Telia, being a virtual monopoly, most of the population of Sweden is included in this register. Telephone subscribers have had no reason to suspect that the register would be used for any other purpose. The same applies to the Motor Vehicle Register and the National Land Register. The Data Inspection Board did not consider that the reasons given justified the creation of a population register for commercial purposes, and Telia's application was rejected.

Yet there is no assurance whatsoever that government on appeal would back up the bureaucratic obstacle put up by the Data Inspection Board. Far from that, there is reason to believe that the commercial profit looks so attractive as to make the government blind to the violation of privacy involved, when government makes money out of its own public files.

4. Circumstances out of control
My last example of limitations I should like to call "Circumstances out of control." Or perhaps rather "One Uncontrollable Circumstance," that is the Internet.

The information once placed on the net is thrown right into the jaws of the monster. Out there, nothing is impossible: searches, cross-matches, storage, manipulation, you name it. But what can I do?

In contrast to some other Privacy Commissioners, my opinion is that the Internet
cannot be regulated. First of all, it can't be done without restricting freedom of expression. That reason should suffice in itself, but there are practical obstacles as well. It is said that today 30 million people in 70 countries have access to The Internet. Assume that I would like to control one of them. What will the other 29,999,999 do in the meantime?

What I can do is spread information on the lack of reliability and on the dangers involved. Failing in an effort to apply regulations to a network building on the very basis of anarchy can only backfire and put in jeopardy the respect the public may have for the Privacy Commissioner.

5. Progress without bureaucracy

What I have said so far concerns the obstacles to the bureaucratic intervention of the Privacy Commissioner. Now the final issue: how can we make progress without bureaucracy?

First of all by co-operation across national borders and working within the European Union, resulting in the EU Data Protection Directive. This Directive applies not just to those of us who are members of the European Union. One Article restricts Member States from releasing personal data to third countries, unless the receiving country maintains a protection level adequate to what is prescribed for EU countries. Therefore, the Directive is relevant to other countries as well, for instance Canada, Japan, and the United States. A unanimous European Union is an economic, and therefore effective, pressure on other countries, to improve their protection of privacy with respect to personal data, and to do so voluntarily.

Another very important element in maintaining the protection of privacy without bureaucracy is effective sanctions. Economic sanctions are, of course, the most efficient ones.

Finally, some visions are in place. Here are some of mine:

1. Introduce strict liability for feeding computers with incorrect personal data.
2. Increase the punishment and lengthen the statute of limitations for crimes against personal privacy. The present low fine should be the exception.
3. Make policemen, prosecutors, and judges learn the laws on the protection of personal data, so that investigations can be finalised before the statute of limitations runs out, and so that improper write-offs are avoided.
4. Put the responsibility for the observance of the law where it belongs - to every activity that includes the processing of personal data. Appoint a Person Responsible for Privacy, just as every firm will have to have a Person Responsible for Environmental Matters. It is to that person one should turn first with questions, not the Privacy Commissioner.
5. The information held in the computer, accessible by more than one person, may always land in the wrong hands. That is why the data fed in must be limited. Only a limited amount and totally necessary data should be allowed to be stored.
6. We cannot limit the flow of information by putting in distinctions between releasing personal data on-line, on diskettes, on CD-ROM, and on paper.
7. The data and the diaries of private citizens can never be checked. So leave them alone, but give them full responsibility for what they let out from their computers.
8. The permit system is obsolete. Let each sector develop its own rules of ethics and check that they are duly observed. Then the Privacy Commissioner will follow up with any necessary inspections.
9. Let us work for a law that builds not on technical procedures but on the basic need for protection. Penal codes normally tell you that you shall not kill. Not that it is forbidden to kill by axe, poison, handgun...

...or by computer. This is a story about the perfect crime. A doctor knew that his wife was allergic to normal general anaesthesia. Before she went into surgery, he entered the computerised journal system of the hospital, using the log of the nurse, and deleted the information on the allergy. When his wife passed away under surgery, her husband had already restored the information in the computerised journal. The operating surgeon, of course, was held liable, and the merry widower inherited his wife's estate.
Hungary adopts new sectoral data protection laws

Before the changes in eastern European political systems in 1989, little or no attention was paid to data protection in former socialist countries, including Hungary. The political and legislative practices in place at the time made no reference to data protection, nor did the citizens have any knowledge of the existence of the concept of data protection. Dr. Kinga Szurday, Data Protection Expert at Hungary’s Ministry of the Interior, explains the legislative changes which have occurred and those which are being prepared.

The Hungarian Constitution was almost completely reformulated in 1989. An important part of the constituent work which laid the foundation for changing the Hungarian legal system was the integration of a guarantee of basic human rights into the Constitution. As a result, the protection of personal data as a fundamental right is now guaranteed to all individuals. Regulations which detail the exact requirements of this guarantee are set out in Hungary’s Data Protection Act (PL&B, Sep 1995, p.3)

Decision number 15 of the Constitution Court in 1991 (PL&B, Dec 1991, p.20) provided an impetus for legislation on data protection. This decision first examined the constitutionality of the personal identification number (PIN) assigned to individuals. PINs were being very widely used without restrictions, and provided legislators with a concrete example of data collection which did not meet the standards of fair information practices. PINs became the basis on which legislators framed an act on data protection.

The data protection framework law

The result was that Act No. 63 of 1992 on the Protection of Personal Data and Freedom of Information (the Data Protection Act) was passed by Parliament in 1992. This Act contains two sometimes conflicting constitutional fundamental rights - the right to protection of personal data, and the right to freedom of information.

In common with the European Union Data Protection Directive, the Hungarian Data Protection Act starts from the principle that personal data should be collected directly from, and with the consent of, the individual to whom it pertains. The individual has the right to know what information is being held about him or her, and has the right to request correction and deletion of personal data. Last but not least, the personal data must be used only for specifically determined purposes.

The Act allows for the compulsory disclosure of personal data contained in administrative registries only where specifically authorised under an Act. Furthermore, the Act sets out instances when the rights of the individual may be restricted, but again, only by statutory provisions. Examples of such instances are where there is a risk to the internal or external safety of the state, national defence, national security, prevention of crime, law enforcement, financial interests of the state or local governments, or the protection of other individuals.

Civil and criminal sanctions

Prevailing Hungarian law contains many civil and criminal sanctions for cases where an individual’s right to personal data protection has been violated. The Data Protection Act enables an individual to bring an action for loss of data protection and to sue for damages. Sanctions are also possible if personal data is being maintained in some unauthorised manner. These sanctions vary with the severity of the unauthorised activity.

Hungary has a Data Protection Commissioner, Dr. Laszlo Majtenyi, who was elected in July 1995, whose role is to ensure that the Data Protection Act is being complied with, and also to examine whether or not the Act provides adequate data protection. The Commissioner’s legal status is identical to that of an ombudsman. He or she has independent constitutional status and is elected by Parliament. Responsibilities of the Data Protection Commissioner include: general supervision of the Act, examination of individual complaints concerning the way that personal data is handled, and the keeping of records pertaining to data protection. This last responsibility is administrative in nature, and has no legal effect.

New sectoral statutes for state records

Hungary’s Data Protection Act identifies compulsory data maintenance as a subject requiring statutory regulation. However, deciding just what data should be maintained has been a
difficult task. Previously, there was no statutory requirement to maintain data, and the result was that there were several systems of records management that were established by secret internal orders. After the Data Protection Act entered into force, the Hungarian government had to review all state administration and jurisdictional records maintained for compulsory data dissemination purposes, and had to enact legislation to provide the required statutory basis for this dissemination.

In the past four years, significant progress has been made in this area. Hungary's government is fulfilling the responsibilities set out in the legislation in two ways. Rules are being laid down concerning the basic administration of records, with regulations being assigned to specific activities in separate Acts.

**Population records:** One of the first steps in this direction, based on the above mentioned decision of the Constitutional Court, was the adoption of an Act which regulates the system of population records and sets out exactly to whom, for what purposes and under which conditions data may be disseminated. This Act allowed the use of PINs until December 31, 1995, and clearly spells out which organisations may use them and for which purposes they may be used.

**Personal Identification Numbers (PINS):** Since the previously mentioned decision of the Constitutional Court, there has been a continuing dispute surrounding the question of the constitutionality of the PIN and the further fate of the system of population records. The administrative system governing population records that is currently in operation was developed in 1972 based on a Swedish model. However, due to lack of technical facilities resulting from the ban of some computer system exports to former communist countries, as information was added over the years, it was not carried out in keeping with the original model. The result is that the population records are now administered under a system which is out-of-date from the standpoint of informatics, and there is no way to ensure that data is updated and current. At the same time, the circle in which this data can be disseminated is much smaller and more restricted than in Sweden.

Before 1991, the use of the PIN was very widespread, especially in banking and insurance. At the same time, it was not used - presumably because of lack of confidence in the system's western origin - in state record systems which belonged expressly to the oppressive structure of the communist system, such as records concerning party members and records dealing with the activities of the internal informant network.

On this basis, it is possible to dispute the commonly held view that the PIN is a symbol of the old oppressive communist system and should therefore be abolished. While the old regime may not have had any system of record keeping and may not have made use of PINs, it is a regrettable historical fact, not only in Hungary but elsewhere, that dictatoral systems violated privacy rights. In the most extreme manifestation of privacy invasion, these regimes took away peoples' lives. Today, it is indisputable, that guarantees and restrictions should be established relating to the use of PINs.

Recently, the Constitutional Court took a position once again on the question of PINs. In the Court's view, privacy rights can be adequately protected by introducing separate systems and different identifying symbols for different branches of government. The Hungarian government is now preparing an Act which makes it possible to separate the three big independent systems currently in existence as well as the identifying symbols assigned to them. The three systems are a system of tax records, a system of social insurance records, and a system of population records. Data files of the latter could serve as a model in the future when applying separate identifying symbols. It is important that managers of the three systems do not know each other's identifying codes. When data dissemination and exchange is required between the systems, it will be regulated by the Act, based on the content of the data and the purposes for which it is required. This draft Act is currently only an outline concept which will be discussed by Parliament in the coming months, and cannot yet be considered final.

**Research and marketing data:** The Hungarian government has prepared a separate draft Act dealing with the use and maintenance of personal data for scientific research, public opinion polls, market research and direct marketing. This Act,

Statistics: Special mention should be made of the Act on Statistics which was adopted by Parliament in 1992. It regulates data protection in the field of statistics in harmony with the recommendations of the Council of Europe.

There are two additional fields where data maintenance will be regulated by separate Acts: health data, and data on criminal proceedings and the regulation of criminal statistics.

Health and criminal data: A draft regulation on the protection and keeping of health data is now ready and Hungary’s Parliament is expected to adopt it this year. Regarding criminal data, partial regulation is still required in areas such as criminal statistics. Other areas are dealt with by the Criminal Code and the Police Act.

Police data: It is important that lawyers dealing in data regulation make a serious attempt to incorporate fair information practices into sectoral Acts. The maintenance of police data has already been regulated in this way based again on the Recommendation of the Council of Europe in the Act on the Police adopted in 1993.

National defence: The Act on National Defence contains important data protection provisions which specify the personal data the defence authorities may collect and process about soldiers and to which institutions or persons this data may be transferred.

Passports: There is also an Act dealing with passports and records related to them. Border guards are currently being prepared with significant data protection responsibilities. In preparing the Act on border guards, Hungary should take into account the Schengen Information System (PL&B, Apr 1996, p.10) on police records relating to people travelling across borders, since it is no secret that Hungary intends to join the Schengen Agreement as soon as possible.

Council of Europe and the EU

Internationally, Hungary’s Secretary of State has signed the Council of Europe Data Protection Convention No. 108 which Hungary plans to ratify after adopting the above legislation.

Moreover, Hungary is paying special attention to the regulatory activities of the European Union in this field. The White Book published by the European Commission - which contains the harmonisation tasks in the field of legislation to be carried out by countries before joining - deals with data protection in a separate chapter. Therefore, it is very important for Hungary to analyse and process the European Union’s Data Protection Directive as early as possible. (In this endeavour, the publications of Privacy Laws & Business have been of great assistance).

Reorganisation of state records needed

Besides legislative responsibilities, the Hungarian government has several additional tasks to undertake. The outdated systems of records must be reorganised in order to satisfy data security requirements, which will requires significant financial resources. In the public administration, this task will be exceedingly difficult as only a small part of the anticipated costs can be met by the budget.

In the private sector, there are not as many obstacles to updating records systems, because private companies can maintain their market position only by keeping up-to-date records. However, public awareness that could force organisations, such as banks and insurance companies, to take data protection rules into account is not yet evident. The state does not plan to interfere with regulation in the private sector, but would like to see self-regulating mechanisms in operation. However, these have not yet taken shape in Hungary.

Need to raise public awareness

Finally, our most important task is to transform the consciousness of our citizens, to enrich their knowledge of their own privacy interests, and to encourage them to protect those interests by taking appropriate steps, such as appealing to a court, where necessary. Active legal protection like this was not practised during the period of socialism. The Data Protection Commissioner has a significant role to help familiarise the public with their rights to have their personal data protected and in raising awareness of their privacy rights.

This report was written by Dr. Kinga Szuردay, Data Protection Expert, Interior Ministry, Budapest, Hungary and edited by Shauna Van Dongen, a Privacy Laws & Business consultant.
US Department of Health appoints a Privacy Advocate

The Office of the Privacy Advocate was established by an administrative decision of United States Department of Health and Human Services (DHHS) Secretary, Donna Shalala, on March 12th 1996. The Privacy Advocate, John Fanning, is an institutional representative and resource for privacy issues with respect to personally identifiable information about individuals in programmes and activities of the DHHS.

The Privacy Advocate reports directly to the Secretary on significant policy matters and in case of conflicts and disputes. The Office of the Privacy Advocate is in the Office of the Assistant Secretary for Planning and Evaluation, within the Office of the Secretary.

This title exists in only one other place in U.S. federal government - in the Internal Revenue Service, where it is held by Robert Veeder. That position is about 2 years old, and is a more established and elaborate position than in the DHHS, because Veeder has staff and can participate in the design of data systems. John Fanning explains his new role.

Policy Consultation and Advice to the Secretary. The Advocate consults with the Department’s component agencies on proposals for new data systems, for programmes requiring new collections of data, and for regulatory and legislative actions necessitating data collection, and advises the Secretary of their implications for personal privacy. The Advocate also independently analyses existing policies and data collections with implications for privacy. But each separate data collection need not be sent for his review and approval.

Membership of the Data Council. The Privacy Advocate is a member of the Data Council, which was formed in 1995 and meets monthly. It co-ordinates all data collection and analysis activities in the Department through development of data collection strategy and co-ordination of data standards, privacy and related policy activities. It is composed of Assistant Secretaries and agency heads reporting to the Secretary, the Senior Adviser to the Secretary on Health Statistics, and the Privacy Advocate.

The Privacy Advocate articulates privacy concerns regarding data policies under discussion, identifies and brings to the council privacy issues, and chairs the Privacy Working Group of the Council. The latter group has representatives from units of the Department, but they do not formally representing their agencies. Their membership is based on their interest and specialised expertise and will change over time.

Technical Assistance and Consultation. The advocate is a source of technical expertise and early consultation on the privacy implications of proposed actions. The Privacy Advocate will maintain reference materials, provide information and refer Department personnel to sources of expertise within or outside the Department. The Advocate is a source of expertise for the Data Council and the National Committee on Vital and Health Statistics, a public advisory committee to the Secretary on health data matters.

Developmental and Resource Functions. The Advocate may conduct or commission research and technical studies on information use and disclosure policies, and may provide training in these areas. At this point, there is no specific privacy budget but the Advocate is in the Office of Assistant Secretary for Planning and Evaluation, through which funds are available. No research has yet been commissioned.

Representation and Liaison. The Advocate is a point of contact and source of information on issues of use and disclosure of personal information for other agencies of government, as well as for privacy and consumer advocacy organisations, private-sector organisations that utilise personal data, the States, foreign governments, and international organisations interested in privacy and data protection matters. The Advocate is a point of public reference and resource for concerns about departmental activities with respect to personal information, and refers inquiries requiring investigation to appropriate units of the Department.

Contact details: John P. Fanning, Privacy Advocate, 440D Humphrey Building, U.S. Department of Health and Human Services, 200 Independence Avenue SW, Washington, DC 20201, USA. Tel: +(1) 202 690 5896 Fax: +(1) 202 690 5882 Internet: jfanning@osaspe.dhhs.gov
The UK Registrar stimulates debate on implementation of EU Data Protection Directive

The UK Data Protection Registrar’s Office does not waste time. Shortly after the Home Office had made public its Consultation Paper on the implementation of the EU Data Protection Directive in March this year (PL&B Newsletter April 1996 p.6), the Registrar issued her own document on this issue.

Provoking debate and response

Entitled Questions to Answer: Data Protection and the EU Directive 95/46/EC, this is a 133 page compilation of separate papers written by the Registrar’s staff on various issues regarding implementation of the Directive in the UK.

The purpose of the document is to stimulate debate and help data users formulate their own responses to the Home Office Consultation Paper. Urging data users to use her paper as a facilitator in responding to the Home Office, the Registrar, Elizabeth France, writes in the foreword to the document: “This is an opportunity that arises once in fifteen or twenty years to influence legislation. Please take up that opportunity.”

In order to assist in preparation of the Registrar’s formal response to the Home Office, data users were asked to send to the Registrar’s Office a copy of their submissions to the Home Office.

Addressing the issues

The Registrar’s Office has produced a comprehensive and detailed document which addresses in depth many issues arising from implementation of the Directive in UK legislation, often speculating beyond the Directive’s provisions into the future. With much thought having gone into drafting it, the document provides worthwhile reading.

Although of somewhat intimidating length and complexity, the document is divided into chapters by subject, hence allowing selective reading and examination. The Chapters are organised as follows:

1. Introduction, including arguments for a seamless data protection law, difficulties arising from a dual data protection regime, the Act as privacy legislation etc.
2. Preliminary Matters, such as scope, automatic and non-automatic processing, boundaries of community law, sensitive data, criminal convictions.
3. The Principles, including interpretation, relationship with the registration system, fair obtaining, Tribunal decision etc.
4. Registration, including functions, requirements, areas of administrative difficulty, timescale and fees, multiple registration, possible methods of implementation, risk and non-risk processing, in-house officials etc.
5. Supervision and Enforcement, including inadequacies in the Registrar’s current powers, investigation, Tribunal, supervisory notices, audit powers etc.
6. Rights of Data Subjects, such as right of privacy, right of access, enforced subject access, right to object, automated individual decisions, compensation, consent, provision of information, judicial remedies etc.
7. Transborder Data Flows, examining transfer prohibition notices, adequacy of data protection in a third country, prohibition of a transfer to third countries etc.
8. General and Miscellaneous, including national supervisory authority, regulation making powers, new technical developments, codes of practice, applicable law, transitional arrangements etc.
9. Exemptions, giving overviews of the Act’s and the Directive’s exemptions and examining future issues such as public interest exemptions, employment/staff planning, personal references, confidential correspondence etc.

Questions to Answer: Data Protection and the EU Directive 95/46/EC may be obtained free of charge from: The Office of the Data Protection Registrar, International Department, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF. Tel: (01625) 545 710 Fax: (01625) 524 510

This report was written by Bojana Bellamy, a Privacy Laws & Business consultant.
Data Protection and the Police workshop papers available

Papers are now available from the Privacy Laws & Business workshop dedicated to data protection issues and the police. The workshop was organised on the day before the official International Data Protection and Privacy Commissioner’s Conference held in September 1995 in Copenhagen, Denmark.

Data Protection Authorities from several countries and interested participants from the police forces, ministries of justice and academia had an opportunity to exchange their experiences and views on some of the current issues in this field, such as specific regulations for police forces, international cooperation, the Europol and Schengen Conventions and the use of DNA profiling for police purposes. To order the following papers and for further information, contact the Privacy Laws & Business office.

2. "The Regulations on the Use of Personal Data in the Police Sector in Denmark" - Registertilsynet (Data Protection Agency).
4. The Netherlands Decree of 14 February 1991 implementing the Data Protection [Police Files] Act (Police Files Decree);
8. “The Schengen and Europol Convention and Data Protection” - Charles Raab, Reader, Department of Politics, University of Edinburgh, UK and Michael Spencer, Consultant/Author, UK.
10. Memorandum of the UK Data Protection Registrar on the Europol Convention;
12. “UK Police Use World’s First DNA Database and Follow Data Protection Rules” - D.B. Gunn, QPM, MA(Cantab), Chief Constable, Cambridgeshire Constabulary, UK.
13. Report by the Privacy Commissioner to the Minister of Justice on the Criminal Investigations (Blood Samples) Bill of February 20, 1995 - Bruce Slane, Privacy Commissioner, New Zealand.

Papers available from the police sessions at PL&B 9th Annual Conference

Police issues will also be on the agenda of the Privacy Laws & Business 9th Annual Conference. Papers will be available. Issues for discussion will include: enforced data subject access requests; regulating third party access to police records; a report on research in Scotland on implementing data protection principles through a code of practice; and the launch of a new police code for England and Wales.