The EU data protection draft directive is now expected to reach a "common position" at the Council of Economic and Finance Ministers on January 16th, 1995 under the French Presidency (January - June 1995). The text would then be forwarded to the European Parliament for a second reading in mid-February. Why was the text not approved under the German Presidency?

By the time the European Commission began its winter break on December 23rd, most Member States were satisfied with the compromises that had been reached on the EU text in the hectic negotiations during and following the Internal Market Council on December 8th. At that meeting, the Ministers were expected to reach a common position. But there were too many remaining points and so the negotiations were handed over to the experts and the Committee of Permanent Representatives (COREPER). The final point of substance was on the rule-making powers of the European Commission. The compromise reached was that the Commission should retain rule-making powers but only over the one issue of transborder data flows to countries outside the European Union. If the Commission wishes to use its powers in any other area, it will have to use the standard procedure it uses for other Internal Market issues. The European Commission will still chair and fund the advisory group of Data Protection Authorities which will give advice to the Commission on any other aspect of the directive which falls within the scope of EU law.

Apparently, the only reason why this compromise failed to be adopted at the Health Council on December 22nd was because of the procedural objection that the item had not been placed on the agenda at least 14 days in advance.

We are now planning the programme for the Privacy Laws & Business 8th Annual Conference to be held 10th-12th July 1995 when we return to St. John's College, Cambridge. Please contact me with your suggestions.

Stewart Dresner, Publisher

CONTENTS

German DPA's revise transborder data flow guidelines ............... 2
UK Registrar gives advice on compliance for document imaging .. 4
Privacy Laws & Business Newsletter subscription form ............ 7
Ontario leads on electronic mail privacy principles ............... 8
France: video surveillance update .................................... 10
How New Zealand regulates data matching ........................... 11
International DPA conference papers published .................... 15
DPA annual reports: Ireland, Canada/What is privacy? ............ 16
Bookends: Corporate policy, OECD, DMA code, Swiss law ........ 20
Worldwide directory of Data Protection Authorities ............... 23
Tables of European Data Protection laws and bills ............... 27

Reproduction and transmission in any form without prior permission prohibited.
Privacy Laws & Business cannot accept liability for any advice given.
Copyright © 1994 Privacy Laws & Business ISSN 0953-6795.
GERMAN DPA'S REVISE
GUIDELINES FOR MANAGING
TRANSBORDER DATA FLOWS

On October 27/28th, the Dusseldorf Circle, the regular meeting of German Lander (state) Data Protection Authorities, revised their checklist of recommended steps to be taken by private sector organisations transferring personal data abroad. The original and revised documents were drafted by its transborder data flows (TBDF) committee, chaired by Dr. Dieter Baumeister, the head of the data protection supervisory authority for Berlin. Their review of the document, published a year earlier, followed mainly negative comments from companies and industry associations. The revised document has not been published but a change was that of description from "checklist" to "guideline." This change indicates that the DPA's now see the document as an interim measure outlining their recommended interpretation of the German Data Protection Act's requirements for transborder data flows, until the EU data protection directive enters into force in national law. The TBDF committee of the Dusseldorf Circle will then revise the document again.

The current legal basis for TBDF

Personal data is transferred in large quantities by private sector organisations from Germany to other countries. Under German law, these transfers are considered as communication to a third party.

The EU Data Protection Draft Directive has not yet been adopted and it will take some time before it is implemented in national law. The question of how to ensure the protection of data subjects' legitimate interests and rights once their personal data crosses national borders, remains open.

The current legal basis for data transfer abroad is the Federal Data Protection Act, § 28 ss. 1 and 2, as well as, § 29 ss. 2, unless sector specific regulations take precedence.

Weighing of different interests needed

The fact that data transfers take place to countries which do not offer a sufficient level of data protection has to be taken into account when weighing the legitimate interests of data subjects, in the context of the above quoted sections of the Act. An agreement between the exporter of personal data based in Germany and the recipient abroad, with the aim of protecting the data subject's rights, does not have absolute value. It is only one of the relevant factors when considering legal requirements for transfers of data abroad.

Such an agreement may be particularly relevant in cases of data transfers:

- without the consent of data subject, and
- which are also not necessary for the fulfilment of a contract with the data subject.

Guideline should reduce data risks

The guideline may be useful in assessing the legality of such transfers. Its aim is to improve the protection of data subjects, which is essential where there are data protection deficiencies in the data recipient's country. It provides the private sector organisations with an instrument for evaluating data transfers.

The guideline should be handled flexibly and according to individual circumstances. The intention was not to set up a fixed model contract, but to adopt additional data protection measures to reduce the risks to the data subject caused by transborder data flows.

The Guideline

1. Co-operation between the data exporter and data importer

The data exporter shall investigate the legal situation with regard to data protection in the recipient country. The first step would be to contact the competent authorities in the recipient country and the data recipient. Then the exporter must assess whether the country has a sufficient level of data protection, by taking into account all elements of the individual case:
• category of data
• purpose, context and usage
• duration of the intended processing
• general or sectoral legal regulations in the recipient country
• codes of conduct in the recipient country.

If the data exporter does not undertake inquiries in spite of the unclear situation in the recipient country, or if the situation concerning data protection still remains unclear in spite of such inquiries, it has to be assumed, if in doubt, that the recipient country does not provide an adequate level of data protection.

2. Purpose and use of the data
The purpose for which the data is to be used should be fixed by the contract in a clear and binding manner. The data exporter and the recipient should agree on prohibiting the use of data for any other purpose. In appropriate circumstances, as a means of clarification, certain inadmissible uses may be cited as examples of prohibited uses.

3. Rights to information
In the interests of the best possible transparency, the data subject should have a right of information with the recipient abroad as well as with the German data exporter. This aim, however, can only be accomplished effectively if the data recipient is bound by contract to provide the relevant information to the sending party. Otherwise, the latter would hardly be in a position to provide the data subject with the information required.

4. Rectification, blocking, erasure
The data subject should have the choice of invoking these rights either against the recipient abroad or against the data exporter based in Germany. Where these rights are used against the sending party, its co-operation is required in fulfilling the duties of the recipient party. This presupposes that the sending party has obtained a right to rectification, blocking and erasure from the recipient party.

5. Notification duty
It is specially important that, beyond the requirements of § 33 BDSG, the sending party is obliged to notify the data subject of the data transfer abroad. In particular, the data subject has also to be informed about the rights he has obtained by the contractual agreement between the sending and the recipient party.

6. Data security
Data security measures should be made a contractual obligation for the recipient. The level of security is primarily dependent on the sensitivity of the data. The data security provision of the German Act (Art. 9), including the Act's appendix, may serve as a starting point for guidance in this respect.

7. Checking the agreement's implementation
The data exporting party must be in a position to check, among other things, the implementation of the contractual agreements mentioned above, in particular:
• the rights of the sending party to obtain or to have access to information and, if necessary,
• rights to on-site inspections by the exporter.

The appointment of a data protection controller might also be worth considering.

8. Penal clause
The data recipient should be bound to pay a penalty to the data sender in the event that the recipient party does not meet its contractual obligations. This too, should strengthen the willingness of the recipient party to observe the rights of the data subject.

9. Liability
The interests of the data subject would receive increased attention if the exporter and the data recipient were under joint and several liability. One might consider a joint and several bond between the exporting and the recipient party, with the data subject being informed about the contents of the contract. Without this, the data subject would not be able to use the rights he obtained, due to his ignorance of them. In cases of transfer of especially sensitive data, a clause on strict liability may also be included.

Privacy Laws & Business is grateful to
Dr Herbert Burkert of GMD, Germany, for translating and interpreting this document.
The draft Guidance Note on Document Image Processing (DIP), published in September 1994, was the first draft policy document issued by the new Data Protection Registrar, Elizabeth France (PL&B September 1994 p.19). In November, Privacy Laws & Business organised two workshops as an opportunity for public and private sector data users to comment and participate in the regulatory process. This report is based on the advice given by Assistant Data Protection Registrar, David Smith, at the November workshops.

Why are DIP systems different?
The major differences between traditional computer data and DIP are that:

1. with traditional computer systems, one should input only relevant information, but with DIP, there is no filter of what goes into the system.
2. with traditional computer systems, one holds information in accessible fields, but with DIP, one holds information at the level of a document.
3. with traditional computer systems, one may delete specific data but with DIP, at least the less sophisticated systems, the user cannot delete specific information in the same way.

The guidance is aimed at the basic systems with the basic level of scanning a document into a computer. However, where possible, data protection guidance should be applicable to the new DIP areas of text/voice/image integration.

The Data Protection Act was introduced because Parliament considered that using computers to process information automatically posed a threat to individuals' privacy. At that time, paper records were not widely seen as a threat. Now, DIP is not only used to save space but also to facilitate retrieval. By applying DIP to manual records, the framework has to be changed and the draft guidance note provides rules to follow to protect the rights of individuals.

Advice 1. In relation to microfiche and microfilm, if there is an automatic way to retrieve the information, then the Act will apply. But if the user has to search manually, record by record, than it will not apply. The ability to automatically obtain information about individuals will determine if the Act applies. An index on computer will come under the Data Protection Act, but a microfiche itself will not.

In DIP systems, the user cannot extract information automatically but only retrieve it. The documents are indexed and can be called up one by one and then be transferred to a traditional computer system.

Registration

Advice 2. The introduction of DIP does not change the registration requirements of the Act as registration is not based on the system in use. The data user does not have to register the fact that he uses DIP. Changes to the registration will be needed if information which data users enter in the DIP is held for an additional purpose or there are new classes, sources, disclosures, etc.

Advice 3. Records held for historical purposes, such as records of the company's activities since its foundation, might be held on a DIP system. The Act does not prevent the holding of such historical records indefinitely, as long as it does not cause damage or distress to the data subject.

Advice 4. In relation to data classes, care must be taken. The user can register for uncategorised information held on DIP for information volunteered in correspondence, as there is no way of knowing what people are going to write. The additional wording in free text might be "information given in correspondence." However, it is not sufficient...
to write "information held on DIP system," as this is not sufficiently descriptive. The Registrar will pay attention if uncategorised information is ticked alone. The company must tick the other fields which relate to the activities of the company.

The Principles

First Principle: Information should be obtained and processed fairly and lawfully

Advice 5. DIP does not change the fundamentals of this principle. There is no need to notify the individual that information is to be held on DIP, as opposed to any other system. The need is to tell him what you do with the information.

Fourth Principle: Personal data shall be adequate, relevant and not excessive

If, for example, a local authority receives a letter from a data subject stating that he is moving and giving his new address, that is the information that the local authority will need. If the individual volunteers more information, in theory, there is no need to record that information. In a traditional computer system, you would key in only the relevant information from the letter as you can select the material for inputting. In DIP systems, this is difficult.

Advice 6. In the above case, the Registrar recognises that, you cannot have control over information which has been volunteered to you in a letter and, therefore, it may be recorded in a DIP system.

Advice 7. When information is given in an application form, the data user has control of what he asks and, before putting it in a DIP system, must check that:

1. the information he is asking for is relevant and not excessive, and
2. the forms are designed to ask for only the necessary information.

The data user must also take care to ensure that he:

1. accurately records the data subject's statement, and
2. can add the date the information was given and a note saying that the information was accurate at the time it was given.

If the information provided is irrelevant or excessive, the data user must re-think whether he needs that information and needs to input the whole document onto the DIP system.

Advice 8. In relation to back files and existing documents, the recommendation given is that if the information is excessive, then do not put the document into DIP, unless the excessive information can be left out. The Registrar recognises that for back files there is a problem as it would be very difficult to start checking old documents.

Fifth Principle: data must be accurate

Advice 9. If the document is inaccurate but has to be retained for some reason, the user needs an indication of that fact. Whatever comes up on the screen must be complete and accurate information, including any note or comment added to the record. For example: "the information on the image was accurate but it has been superseded by new information."

Advice 10. If a document relates to third party information or information filled in on behalf of the company by third parties, it must state who recorded it and the date it was recorded. The date on the document determines which is the most up-to-date record.

Advice 11. In the case of a medical diagnosis, the Act will not require the removal

---

Data Protection Manager Looking for New Role

A UK data protection manager with information systems strategy experience is looking for new opportunities. He is currently the data protection manager for an organization employing 22,000 people with £450 million in annual turnover. He would prefer a West Midlands location.

For further information, please contact the Privacy Laws & Business office.
of the information from the record if it could be important for future medical reasons.

Sixth Principle: personal data should not be kept for any longer than is necessary

For example, an organisation may only need the date of birth of people until a certain age; after that, the information is not necessary. Here, the Registrar takes the same view as for the fourth principle.

Advice 12. If information is volunteered, then there is no way of controlling it. Thus, the document can be kept for as long as it is necessary because some information on it is relevant. However, if you ask for information, such as date of birth and this information is not necessary after a certain date, then you have to design the form or the system in a way to get rid of such information at the appropriate time.

Advice 13. For back files, the recommendation is to add a reminder date which will alert the user when it is time to review the information.

Advice 14. Information that has to be kept for long periods of time for legal reasons. The Registrar is reluctant to accept that because of an unforeseeable future reason, you might need to keep information forever. If an organisation can provide a good reason such as mortgage, finance, or money laundering regulation, then this should be acceptable. Legal requirements are not questioned by the Registrar.

Seventh Principle: Data subject access

Advice 15. Data subjects have a right to a copy of all information about them which is held on a DIP system, including opinions for references. On opinions, the Data Protection Act does not empower an individual to challenge accuracy and you may withhold the identity of the person who gave the opinion. Where another data subject may be identified by the disclosure of information, the identity of that individual may be withheld.

Eighth Principle: Security

Advice 16. Security requirements are the same for DIP as for any conventional system.

DOCUMENT IMAGE PROCESSING USERS’ WORRIES ABOUT THE GUIDANCE NOTE

Many of the 1,000 members of Cimtech (the Centre for Information Management and Technology, a document management trade and user organisation), use DIP. Their worries about the DIP draft guidance note relate to three areas:

1. The impact in general on system design, functional requirements and system specification. Potential users may need to upgrade the design of their DIP system and this may increase costs. Where users already have DIP systems, they may need to change the design which may equally incur higher costs. For example, where documents may be currently indexed on a case basis, they may, in future, need to be indexed on a document basis.

2. The problem of back file conversion and how to deal with old information stored on microfilm and/or paper.

3. The problem of legal admissibility and possible conflict between the Data Protection Act and the work being undertaken in this area by the British Standards Institution (which has produced BSI standard 7768), the Legal Images Initiative and a collaborative effort by the Document Management Suppliers Group (DMSG) and the UK Association of Image and Information Management (UKAIIM, a division of CIMTECH). All of these groups are distinct. The concern which CIMTECH has is that the standards, codes of practice and guidelines produced by these groups may conflict with the guidance note produced by the Data Protection Registrar. This conflict applies, in particular, to the issue of certification. BSI 7768 requires that DIP operators will have to certify that they have input the original documents and that they have not tampered with them. However, the Data Protection Registrar requires that certain data is deleted before inputting it into a DIP system, for example, if it is inaccurate.
Physical control, different levels of access control to the document, and audit trails should be in place, among other things. In relation to access control of a computer bureau, it is subjected to the same security requirements as the data user who contracted them. The Registrar might investigate an agreement between the bureau and the contractor.

**Enforcement**

In the draft guidance note, there is an outline of the breaches which may occur.

**Advice 17.** If there is a breach of one principle, the Registrar will look into it, if there is a complaint, and will advise accordingly, for example, to delete an inaccurate record. Only in extreme cases of breaches of principles, might an enforcement notice be issued and a change on the system might be required.

*The Registrar’s criteria for taking enforcement action* will include looking into the specific case and assessing:

1. whether there was damage or distress
2. the sensitivity of the data
3. the number of individuals affected
4. how long the data is being held and what efforts the company has made to comply with the Act.

**Advice 18.** With the guidance in place, whoever installs a new system will have to comply. A less rigorous view might be taken towards old systems and back files. However, the Registrar would like to see one set of rules applied to old and new systems. Perhaps data users with old systems will have more time to adjust, as has been discussed for the provisions related to manual records in the EU data protection draft directive.

A fuller version of this paper, with examples of anonymised participants' experience of data protection problems related to DIP, and the participants' recommendations to the Data Protection Registrar, is available from the *Privacy Laws & Business* office.
ONTARIO GIVES LEAD ON ELECTRONIC MAIL PRIVACY PRINCIPLES

Responding to the extensive use of electronic mail (e-mail) and its potential threats to privacy, Tom Wright, Information and Privacy Commissioner of the Canadian province of Ontario, has developed a set of privacy protection principles for the use of e-mail systems. The principles are specifically addressed to provincial and municipal government organisations under the jurisdiction of Ontario's Freedom of Information and Protection of Privacy Act. However, they are useful for both public and private sector organisations in developing and implementing their corporate policies on e-mail worldwide.

E-mail is a paperless form of communication which allows messages to be sent from one computer user to another. Within and between the organisations, e-mail can be an effective tool which helps break down barriers to communication and promotes the free exchange of information and ideas. On the negative side, however, as noted by a data security expert, e-mail has "the same security level as a postcard." In addition, e-mail creates an electronic trail of messages that can be used to monitor individuals. Complex legal and ethical questions have emerged about the right to privacy of e-mail users, particularly in the workplace. Enhanced communication can make the organisation run much more effectively and efficiently. However, employees will only make use of e-mail to the extent that they feel comfortable that what they transmit will remain, for the most part, confidential. Management's efforts towards employees' privacy will enhance the quality of worklife and encourage employees to use e-mail to its fullest potential.

The following privacy protection principles are intended to provide a framework for developing and implementing more specific policies on e-mail.

1. The privacy of e-mail users should be respected and protected

A survey of managers in the USA indicated that searching of e-mail files is one of the of employee monitoring. While employers may argue that electronic monitoring helps to increase productivity, research indicates that it can actually have an adverse effect on productivity.

Although it is not possible to guarantee complete privacy in relation to e-mail, it is in the best interests of an organisation to offer the highest degree of privacy possible. One of the advantages of e-mail is that it has democratised the workplace by breaking down barriers to communication between different levels of hierarchy. Enhanced communication can make the organisation run much more effectively and efficiently. However, employees will only make use of e-mail to the extent that they feel comfortable that what they transmit will remain, for the most part, confidential. Management's efforts towards employees' privacy will enhance the quality of worklife and encourage employees to use e-mail to its fullest potential.

2. Each organisation should create an explicit policy which addresses the privacy of e-mail users

Every organisation should develop a formal policy on e-mail privacy. Every individual within the organisation should be made aware of his/her rights and obligations under the policy and agree to adhere to it.

The policy should be developed jointly by representatives of employees, managers, personnel, legal and IT departments. Participation of the e-mail users in the development and implementation of the policy is a key element in fostering commitment. Also, education and training will be necessary to ensure that the policy is properly implemented.

The policy should, as a minimum, set out the following:
- purposes for which the e-mail system may be used
- conditions and procedures for access to e-mail by third parties
- consequences of breaches of the e-mail policy.
3. Each organisation should make its e-mail policy known to users and inform them of their rights and obligations regarding the confidentiality of messages on the system

   It is important that every employee is expressly informed about his/her rights and obligations regarding the use of e-mail in the workplace. It may not be sufficient to simply have the policy set out in the corporate manual. Each employee should read the policy and agree to abide by it. Also, training on how to implement the policy should be provided for both managers and employees. Finally, updates to the policy should be made in a manner which ensures awareness on the part of all staff, for example, at meetings, through a newsletter, and via e-mail.

4. Users should receive proper training regarding e-mail and security and privacy issues surrounding its use

   Due to a lack of awareness, e-mail users often assume that their communications are private.

   "The more users know about e-mail systems, the better they will be able to protect their own privacy and the privacy of others. Users need to understand the following about e-mail systems:
   1. the e-mail process is not inherently private
   2. a message does not necessarily disappear when it is transmitted
   3. deleting a message from one's personal files does not necessarily delete all copies of the message
   4. electronic files can be readily transferred
   5. electronic mail systems may be networked to provide connections to other organisations or individuals, or to public access points
   6. the addressee may not be the only person who reads the e-mail
   7. copies of messages are not necessarily duplicates of the original [as a message can be altered before being forwarded]
   8. people can break into e-mail systems
   9. e-mail technology may work against privacy
   10. e-mail can be monitored from a remote location without any indication that the monitoring is occurring
   11. use of e-mail at remote sites may result in the creation of records that the organisation has little control over
   12. not all e-mail systems automatically encrypt files and messages
   13. wireless systems are more vulnerable to unauthorised interception of e-mail messages than other systems."

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

   The privacy rights of both e-mail users and individuals who are the subjects of e-mail messages must be addressed. When personal information is exchanged via e-mail, several features inherent to e-mail systems may contribute to breaches of fair information practices required by Ontario's privacy law. The ease with which personal information may be exchanged via e-mail, both intentionally and inadvertently, may facilitate the unnecessary collection and inappropriate or unauthorised use and disclosure of personal information.

   Although the originators of e-mail messages may carefully adhere to their information practices in disclosing personal information to others via e-mail, they may have no control over how that information is subsequently used or disclosed by recipients. Also, since recipients of personal information may not be aware of the original purpose for which the information was collected, they may inadvertently use or disclose the information for an inconsistent purpose. The further removed the personal information becomes
from the original source, the more difficult it becomes to adhere to fair information practices.

6. Providers of e-mail systems should explore technical means to protect privacy

There are some technical measures which can be incorporated into e-mail systems to enhance privacy protection for users and other individuals who are subjects of e-mail messages.

The first line of defence against unauthorised access to e-mail is user identification through a unique identification number, bar code cards or smart cards and authentication through the use of passwords, hand prints or voice registration.

Encryption is another important technical means of protecting privacy. However, even if a local e-mail system is capable of encryption, the messages which are transferred to a public e-mail system are vulnerable to interception, as encryption is not usually available with public systems.

Other privacy protection features include the capacity to conceal the subject of a message and a warning that a message requiring special security has been received. Also, automatic log-off from the system, whenever the computer is inactive for a specified period of time, is another security feature which will help to prevent unauthorised access to e-mail.

Each organisation should examine its own security needs and select a system which is most appropriate for itself. An organisation's needs for security may vary depending on the type of information that is transmitted and received via e-mail.

7. Organisations should develop appropriate security procedures to protect e-mail messages

Technical features and privacy protection policies regarding e-mail will only be effective to the extent that they are accompanied by appropriate procedures to ensure the security of files and messages transmitted and received via e-mail.

This shortened version of the Ontario Information and Privacy Commissioner's report was edited by Bojana Bellmay, a Privacy Laws and Business consultant.

The full text of the report Privacy Principles for Electronic Mail Systems published by Tom Wright, Information and Privacy Commissioner, Ontario is available from his office. See page 25 for contact details.

FRANCE: VIDEO SURVEILLANCE UPDATE

Mme Louise Cadoux, vice president of the CNIL, France's Data Protection Authority, has called PL&B to give further information on our recent report (PL&B October '94 p. 17) on the CNIL's jurisdiction over video surveillance.

She stresses that CNIL claims jurisdiction over both digital and analogue video images captured and stored by any device. If a video image of a person is stored at all, the CNIL claims competence.

As stated in our report, the Senate debated the Public Security bill on November 8th and improved the text. However, the Senate rejected the CNIL's view of the extent of its competence over video surveillance.

A minimum of 60 members of the National Assembly may make an appeal to the Constitutional Court against this decision. But in the past, the court has said that a new law may modify the scope of a previous law. Therefore, the CNIL's view is unlikely to prevail along this route.
Throughout the world, governments are taking an increasing interest in adopting information matching programmes, sometimes known as data matching or computer matching, to increase efficiency and reduce fraud. While these goals are worthwhile in terms of ensuring that public money is properly spent, data matching programmes often raise questions of how far they should go in intruding on individuals' privacy.

A typical programme involves matching tax data with social security claimants. Should data matching be carried out on a mass scale or be restricted only to suspected fraudsters? What are the costs of the programme compared with the amount of money saved as a result? To what extent do the programmes have a deterrent effect? Do the financial benefits outweigh the costs in terms of privacy? To what extent are such programmes leading to an unacceptable degree of surveillance?

It is often the Privacy Commissioners who are in the lead in trying to strike a balance. Having spoken to a number of Privacy Commissioners from several countries and on reading DPA annual reports from other countries, it is clear that the issue is a high privacy priority in many societies. To discuss the issue, Privacy Laws & Business organised a workshop mainly for Data Protection Authorities (DPA's) on the day before the International Data Protection Commissioners' Conference in the Netherlands in September, to enable the DPA's to exchange their experience and views. At this workshop, one of the contributions which attracted the closest attention was that of the New Zealand Privacy Commissioner, Bruce Slane. He has specialised experience because the law which established his office was aimed primarily at regulating data matching. This is his report.

1. The controls on data matching

Even before New Zealand's Privacy Act was brought into law in 1993, there were some controls put on information matching activities by the Privacy Commissioner Act 1991. That first Act set up my position and essentially required me to exercise a watching brief, reporting and recommending to government on privacy issues and the content of anticipated further legislation which was to incorporate into New Zealand law the OECD privacy principles. It also imposed specific controls on information matching activities between different government departments. At the same time, a number of other statutes which dealt in one way or another with information matching in the public sector were amended to provide the legal authority for those activities to be controlled by the Privacy Commissioner Act. The information matching controls of the 1991 Act were carried forward more or less unchanged to become Part X of the Privacy Act 1993 under which I now operate.

An "information matching programme" is defined as being the comparison by manual or electronic means of any one document containing personal information about 10 or more individuals with other such documents, for the purpose of producing or verifying information that may then be used to take adverse action against an individual. "Document" is widely defined so that it can refer to a computer record. The Act then lists, by reference to other statutes, certain information matching programmes which are "authorised" and it requires that every authorised information matching programme must be conducted in accordance with a written agreement which in turn must be in accordance with a set of information matching rules contained in the Fourth Schedule of the Privacy Act. A copy of every written agreement for these programmes has to be sent to me, and the agencies who carry out these programmes have to report to me in a regular and formal way on the information matching programmes which they have been conducting.

The information matching rules require detailed technical standards to be established to
govern the operation of the programme, and they prohibit any "on-line" transfers of information in these programmes without my express approval. The rules require reasonable procedures for the confirming of any discrepancies found before any adverse action is taken against the individuals concerned. No adverse action is to be taken unless the individual has first been sent written notice which specifies the discrepancy found and gives five working days in which to challenge or explain the discrepancy. There is an exception to this requirement of advance notice where it would prejudice an investigation into the commission of an offence.

In very broad terms, the New Zealand legislation sets out to control information matching programmes in the following ways, to:

- prevent the automatic updating of one database from another
- give the individual affected the chance to challenge the accuracy or the meaning of a discrepancy before adverse action is taken against her
- instil formal standards and procedures for the operation and checking of these activities
- require the organisations which carry out these programmes to report on the operations, their procedures, the costs incurred and results obtained
- require the destruction as soon as practicable of all personal information which has been disclosed or assembled for information matching purposes
- prohibit the creation of any new databank of the information used in or created by the information matching programme.

Above all, perhaps, the requirement that the agencies report to me upon their information matching activities, and that I in turn report publicly and at least annually on those activities, means that they are exposed to a considerable degree of parliamentary and media scrutiny.

Additionally, I am required to examine and advise on any new legislation which proposes further information matching activities. In doing so, I am obliged to have regard to certain matters including the public importance of the objective indicated for that programme, the need for such a programme to achieve that objective, and the balance between the public interest in allowing the programme and the public interest in the privacy rights affected by it. Every five years I am required to review the operation of every legislative provision which permits information matching activity and report to the Minister of Justice on whether or not I consider that the provision should continue or should be modified. The Minister is required to lay my report before Parliament.

2. The use of data matching

Information matching in New Zealand has so far been used predominantly by the Social Welfare agency to detect cases of over-claimed benefits. Regular programmes compare lists of benefit recipients with lists from:

1. the income tax agency showing new starters in employment,
2. the customs agency showing people leaving the country to travel overseas, and
3. the education agency of students getting grants for being in full time tertiary study.

A new programme is just about to start comparing the list of benefit recipients with those who are in prison!

Another being planned is to compare the people receiving a family support payment as a tax credit against their employment earnings and those receiving the corresponding benefit as a social welfare payment on the grounds that they don't have any earnings.

All of these are examples of situations where the same individual should not be on both lists unless some express exception has been made, and that is the only type of matching programme which is presently being carried out in New Zealand.
Substantial financial savings?

Even the few information matching programmes which I have examined have shown some characteristics which I gather are common in other countries. First, there is a tendency to justify the introduction of each new programme by pointing to substantial financial savings, and to confirm those savings by under-reporting the costs involved and by over-estimating the financial results.

Typically, the costs reported have failed to pick up the time involved in checking apparent discrepancies and chasing detected over-payments. Usually, the claimed savings have assumed that all over-payments identified will be fully recovered from the individuals concerned, and have also assumed that if the over-payment had not been detected by the information matching programme, it would have continued at the wrong rate for a long period into the future.

I don’t think that these cost and saving distortions are deliberate; it just happens that the most accessible figures and estimates all tend to distort the truth in the same direction. There is no obvious incentive for the agency itself to devote extra efforts to get more and better information. When I have pointed out the doubtful nature of the figures, the agencies have quite readily accepted my points and have then tended to justify the programme more on the grounds of fairness and the deterrence of cheating than on the grounds of demonstrable monetary savings.

Accuracy of the apparent discrepancies?

The second area of concern for me has been the accuracy or reliability of the apparent discrepancies thrown up by the information matching programmes. I know that some of the staff in the agencies concerned have been unpleasantly surprised by what they have discovered about the accuracy of their own data from trying to compare it with that from another agency.

It is because of the potential for such inaccuracies that the Privacy Act requires the sending of a warning notice to the individual concerned before adverse action is taken. However, it is still very undesirable for people to receive such warning notices when they have done nothing wrong or - even worse - when the information which generated the apparent match was clearly wrong. I can illustrate this by using some figures from the New Zealand experience.

In the year ended 30 June 1993, there was a regular weekly "run" of an information match between the details (supplied by Customs) of people departing from and returning to New Zealand through the country’s various international airports, and the details of the people who receive various social security benefits. There would have been about 3,800,000 passenger movements and half of those would have been departures.

During the year, 8,943 social welfare benefit recipients were spotted as being in both lists and were sent notices telling them that they had to explain matters, otherwise their benefit would be withdrawn. In 6,584 cases there was an "adverse action" taken, which probably meant stopping the benefit and creating a debt back to Social Welfare of the overpaid benefit. Those are the Department of Social Welfare’s own figures.

What I see as significant is that apparently 2,359 (which is 26%) of the people who received these notices were able to respond and convince the Department that no action ought to be taken against them. All of those people were subjected to alarm, annoyance and inconvenience for perhaps no good reason at all, and this is a "cost" which is never taken into account in looking at the costs and benefits of an information matching programme such as this.

When Departments who carry out information matching programmes report to me on the overpayments which their programmes have detected and established, I require them to give some breakdown of the total monetary figures. I have asked for median, upper and lower quartile figures. For over a year, they have been telling me that they were not able to give those figures until they had developed a
new reporting procedure or written some new computer programs.

The Department of Social Welfare claims that benefit over-payments totalling over NZ$11,200,000 were established from the matches with Inland Revenue of returns put in by employers. They say that:

- just NZ$2,000,000 of that was recovered during the year.
- The over-payments were detected in respect of 13,814 people, and this was out of over 87,000 apparent matches which remained unexplained after their "quality checks". They have not yet given me the number of the warning notices which were sent out.
- The largest single over-payment detected was $73,000, the smallest was 48 cents.
- The upper quartile was $1,403, the median was $230 and the lower quartile was $85.

I think this shows that it is worthwhile to look for the details behind the total savings figure of $11 million.

3. Conclusion

Information matching is an attractive weapon to use in what has become a battle to lower government welfare spending and to detect welfare cheats. It looks at first to be a clean and precise weapon which will pay for itself many times over, and that is the justification normally given for using it over the complaints of the privacy advocates. We are still learning in New Zealand about how to control this weapon, but I am finding that it is neither as sharp nor as cost-effective as many people have thought. Like many initiatives which impact upon individual privacy in the name of the public good, it is perhaps a technological fix attempting to deal with a broader social problem.

I am pleased to say the present New Zealand government seems committed to being open about the use it makes of information matching. It has also insisted that departments obtain specific statutory authority for Parliament for any new information matching proposals.

In my function of monitoring and periodically reporting on existing matching activities and reporting on new proposals I will be aiming a questioning spotlight into its more doubtful corners.

This edited paper was delivered by Bruce Slane, Privacy Commissioner, New Zealand, at the Privacy Laws & Business Data Protection and Data Matching Workshop which took place in the Hague, the Netherlands, September 5th, 1994. The workshop papers are available from the Privacy Laws & Business office.
DPA CONFERENCE PAPERS NOW PUBLISHED

In September, the proceedings of the 15th International Conference of Data Protection and Privacy Commissioners, held in Manchester, 27-30 September 1993, were published on the retirement of the host, the UK's Data Protection Registrar, Eric Howe. The papers include:

Freedom of Expression and Privacy Protection
- Privacy and the press, David Eady QC, Calcutt Committee Member, 1989-90, UK
- Freedom of expression and privacy protection, Keith Parker OBE, Editor, Express & Star, Wolverhampton, UK
- Liberté d’expression et protection de la vie privée, Alex Turk, Sénateur, CNIL, France
- Freedom of expression and privacy protection, George Apenes, General Director, Datatilsynet, Norway

Identifying and Labelling People
- Balancing risks and benefits in personal identification systems, David Flaherty, Info. & Privacy Commissioner, BC, Canada
- Is it a sin to use a PIN? Anitha Bondestam, Director, Data Inspection Board, Sweden
- Who should know what is written in my genes? Dr Tom Wilkie, Science Editor, The Independent, UK
- Privacy implications of genetic testing: Australian developments, Kevin O’Connor, Privacy Commissioner, Australia
- Labelling people - the threat to civil liberties, Andrew Puddephatt, General Secretary, Liberty, UK

Collecting and providing information about people
- Social costs and benefits of the census, Professor Stan Openshaw, Professor of Human Geography, University of Leeds, UK

Surveying People
- Big brother is watching - video surveillance in public places, John Burrow CBE, Chief Constable, Essex Police, UK
- Location information for simplifying computer applications and communications, Dr Andy Hopper, Director, Olivetti Research Laboratory, UK
- Television and data protection - the example of reality TV, Dr Hans-Hermann Schrader, Commissioner, Der Hamburgische Datenschutzbeauftragte, Germany

International Developments in Data Protection
- Public reaction to the Hong Kong proposals, The Hon. Mr Justice Mortimer, Chairman, Law Reform Commission, HK
- EC directive update, Paul Waterschoot, Director of Directorate E, DG XV, Commission of the EC, Belgium
- International developments in data protection in OECD countries, Christian Schricke, Legal Counsel, OECD, France

A copy of the proceedings, entitled All About People, (173pp) is available from the PL&B office with permission of the Office of the Data Protection Registrar. Price £25.
IRELAND'S DATA PROTECTION COMMISSIONER'S ANNUAL REPORT 1993


This is the first annual report to be prepared by Commissioner, Fergus Glavey, who was appointed in September 1993. He covers:

- raising awareness, for example, "awareness weeks" in different towns which included public lectures, radio and television interviews, leaflet and poster distribution and the establishment of information stands in main shopping malls; the launch of a public survey on public perceptions about data protection; and promoting awareness of the law to data controllers,
- dealing with enquiries (about 50% of enquiries were about credit information) and complaints (24 formal complaints in 1993 against both public and private sectors),
- registration (he warns of stronger enforcement action against those who refuse to register),
- the expectation of codes of practice to cover direct marketing, insurance and credit information.

The report also includes a section on international developments, namely the EU Data Protection and ISDN Directives and inter-governmental conventions in the area of police, customs and judiciary co-operation.

In the second part of the Report, the Commissioner discusses on-going policy issues, in particular:

- the refusal by the Revenue Commissioners to grant a right of access by an individual to data on himself on the grounds that the giving of such access would prejudice the collection of tax revenue,
- pressure to extend the use of an individual's Revenue and Social Insurance (RSI) number for other purposes and the rules which should apply to the transfer, access and matching of personal data between one government department/agency and another, and
- his views on the future shape of data protection and related legislation.

He sums up his view of the law which is "the belief that the individual's rights lie at the heart of our data protection system and should be a significant factor in evaluating the weight to be given to any competing rights which may arise."

Tel: + (353) 1 874 8544
Fax: + (353) 1 874 5405

CANADA'S PRIVACY COMMISSIONER'S ANNUAL REPORT 1993-94

Nothing less than broad privacy legislation - for both government and business - will ensure Canadians hang on to their privacy in the face of the information highway. This is the main message in Canada's Privacy Commissioner's Annual Report 1993-94. "Without some rules, the first roadkill...will be our privacy and dignity...No longer is it sufficient to talk about protection privacy with sectoral codes, self-regulation, patchwork legislation and industry watchdogs," warns Bruce Phillips, Canada's Privacy Commissioner and urges nation-wide privacy protection rules for both public and private sectors.

Consumers are finding financial institutions monitoring their cheques; video stores pressing them for family income; and a long distance telephone service demanding their tax number. New information systems also promise consumer banking, shopping and government and medical services from home. These...
systems will collect and record not just individual transactions but the patterns of those transactions. "Without any rules - and there are no rules in the private sector, except in Québec - Canadians could find their behaviour monitored and data manipulated, used and sold for purposes they neither envisaged nor intended."

The report refers to sectoral codes, in particular:

- the Canadian Direct Marketing Association's Code ("While it lacks an independent arbitrator to handle complaints, it restores considerable control to those who want to stop the mail and marketing calls."),
- The Telecommunications Privacy Protection agency ("appears to have been stillborn."),
- The Canadian Standards Association's continuing work on drafting a model private sector code,
- The Canadian Bankers Association code (and those of the individual banks) do not cover subjective information about individual clients nor do they protect bank employees. "broad disclosures are allowed to serve the banks' business interest.... And the codes will do nothing to prevent banks exchanging clients' personal information with the insurance companies and stock brokerages they may now own...."

"Each of these privacy solutions addresses only part of the problem. New communications networks will be shared by governments, most of which live by privacy codes, and private sector, most of which is unregulated."

The report lists some "privacy considerations that need explicit recognition on the Information Highway.

- Set out in law a fair information practices code to govern the highway,
- Give individuals control over the personal details that are transmitted on the highway,
- Assure individuals that the information will go when and were it is intended - the confidentiality of electronic communications must be protected,
- Limit the collection of personal information to the details essential to providing the service,
- Do not disclose personal information without the individual's explicit consent, and explain data collection practices to clients,
- Protect transactional data (the record of how and when individuals use the system.) Do not gather and use transaction patterns for other purposes without the individual's consent,
- Develop cryptography and other technical and security measures to protect the privacy of electronic communications,
- Do not charge for privacy protection,
- Government must accept an oversight role to monitor privacy protection on the highway".

The Commissioner in his Annual Report also discusses several other trends and issues, such as data matching, ID cards, health records and smart cards. This section of the report covers the creation of a federal government Blueprint for an integrated electronic system to deliver its information services. "Not only would federal agencies create and manage shared personal databases, the Blueprint also envisages sharing the information with provincial governments and the private sector (which, except in Québec, has no built in privacy protections)....How will governments reconcile sharing personal databases with that fundamental privacy tenet - collecting only the minimum personal details needed to administer a program? There follows a number of specific privacy questions and the section concludes with the observation that "shared personal databases threaten becoming the single government computer file that privacy laws were enacted to prevent."

During the year, the Privacy Commissioner's office also:

- received 1,290 new complaints and found just under 40% were well-founded,
• handled 8,688 inquiries and publication requests, and
• carried out seven departmental audits, 13 follow-up reviews of earlier audits and 12 incidents of lost or improperly disclosed personal information.

Annual Report 1993-94, Available from:
Privacy Commissioner of Canada, 112 Kent Street, Ottawa, Ontario K1A 1H3, Canada. No charge. This publication is also available on audio cassette.
Tel: + (1) 613 995 2410
Fax: + (1) 613 995 1501

British Columbia’s Information & Privacy Commissioner’s Annual Report 1993/94

David Flaherty, the Information & Privacy Commissioner (IPC) for the Canadian province of British Columbia (BC), has published his first Annual Report 1993/94. The Freedom of Information and Protection of Privacy Act was proclaimed on October 1993, but David Flaherty was appointed as British Columbia’s first IPC in July, 1993. The law covers all BC government ministries, and over 200 provincial government corporations, boards, commissions, and agencies.

The report mentions special features of the Act which have received favourable comment which include:

1. the strong statement of information rights and the duty of government to assist applicants requesting records,
2. the powers given to the BC IPC to ensure that government meets its responsibilities under the legislation, particularly the Commissioner’s powers to order cessation of inappropriate personal data collection and disclosure,
3. the publication of a public records index which will list those government records which are available without a request for access under the Act,
4. the fact that harm must be demonstrated before information can be withheld under the freedom of information part of the law,
5. the limitation of exceptions or assignments of time limits on exceptions,
6. a strong and usable public interest override which applies to all exceptions and can be used even without a request;
7. protection against the use of personal information for mailing lists or solicitations by telephone or other means.

The Annual Report provides the background to the Act and explains the role of the Commissioner and the mandate of his Office (see box on next page). It also contains summaries of selected reviews and complaints. Since the enactment of the Act, the Information and Privacy Commissioner’s Office has opened 275 cases. The majority of these cases were closed through mediation and only six were referred to the Commissioner for an inquiry.

In October, 1994, the Act was extended to include local public bodies, such as municipalities, schools and school boards, local police forces, health care providers, colleges and universities. In the spring of 1995, the law will apply to the self-governing professions.

BC IPC’s Annual Report 1993-94.
Available from: Crown Publications,
521, Fort Street, Victoria, British Columbia, B8W 1E7, Canada.
Tel: + (1) 604 386 4636
Fax: + (1) 604 386 0221

Manitoba’s Ombudsman’s Annual Report 1993

Privacy Laws & Business has received the 1993 Annual Report of the Ombudsman of the Canadian province of Manitoba. The province’s Freedom of Information Act was passed in July, 1985 and provides for a general right of access to records in the custody or control of a government department or agency. The Act mentions the protection of personal
privacy as an exemption to disclosure and does not regulate the responsibilities associated with collection, storage and use of personal data.

The weakness of Manitoba's law regarding privacy has recently become apparent. The contract for the computerization of health records was won by a company owned by a bank which is subject to no privacy law in Manitoba.

Available from: Ombudsman Manitoba, 750-500 Portage Avenue, Winnipeg, Manitoba, Canada.
Tel: + (1) 204 786 6483
Fax: + (1) 204 942 7803

WHAT IS PRIVACY?

David Flaherty, British Columbia Commissioner explains the meaning of privacy. His "sense of the particular privacy interests of individuals in information about themselves includes the following considerations:

- the right to individual autonomy
- the right to be left alone
- the right to a private life
- the right to control information about oneself
- the right to limit accessibility
- the right of exclusive control of access to private realms
- the right to minimize intrusiveness
- the right to expect confidentiality
- the right to enjoy solitude
- the right to enjoy intimacy
- the right to enjoy anonymity
- the right to enjoy reserve
- the right to secrecy.

With respect to specific data protection principles and practices for government personal information systems, the following list incorporates the main considerations and values that my colleagues and I are trying to promote in British Columbia:

1. The principles of publicity and transparency (openness) concerning government personal information systems (no secret data banks).
2. The principles of necessity and relevance governing the collection and storage of personal information.
3. The principle of reducing the collection, use and storage of personal information to the maximum extent possible.
4. The principle of finality (the purpose and ultimate administrative uses for personal information need to be established in advance).
5. The principle of establishing and requiring responsible keepers for personal information systems.
6. The principle of controlling linkages, transfers, and interconnections involving personal information.
7. The principle of requiring informed consent for the collection of personal information.
8. The principle of requiring accuracy and completeness in personal information systems.
9. The principle of data trespass, including civil and criminal penalties for unlawful abuses of personal information.
10. The requirement of special rules for protecting sensitive personal information.
11. The right of access to, and correction of, personal information systems.
12. The right to be forgotten, including the ultimate anonymization or destruction of almost all personal information."
"Managing Privacy: Information Technology and Corporate America" - H. Jeff Smith

This book provides the reader with a number of valuable insights into privacy policies and practices, as well as attitudes, of major US corporations. The study is based on interviews and questionnaires with representatives from several banks, health and life insurance organisations and a credit card issuer. The book has grown out of the author's doctoral thesis at the Harvard Business School.

The author concludes on the great sensitivity of privacy protection to many industries: "Executives were often unwilling to discuss their own companies' policies and practices or to subject them to the scrutiny of research."

The study revealed that although everybody agrees that personal data has become a valuable commercial property, many companies lack comprehensive policies regulating access to and distribution of the personal data they have collected. Even where stated policies do exist, actual practices often conflict. Furthermore, different divisions within a single organisation often have different perspectives on the importance of privacy protection.

Few organisations are willing to become leaders in developing privacy protection policies. Instead, they reassess and reform their practices only as a result of pressures from consumers, media or legislation.

The author suggests a way forward for US corporations:

- a short-term audit to establish and evaluate the existing "privacy environment" and
- a long term programme for maintaining a healthy "privacy environment."

He believes that a "decision on how the USA will address privacy problems in the future lies to a great extent in corporate hands: will they (the organisations) voluntarily address the problems in a responsible fashion or will they force legislators to do it for them?"

Apart from industry initiatives, the author also believes in and advocates the establishment of a Data Protection Board and a set of "generally accepted privacy principles."

H. Jeff Smith is Assistant Professor of Business Administration at Georgetown University, Washington, USA.


$17.95 paperback, $45 hardback. Tel. +(1) 919 966 3561

The OECD report on privacy and data protection

The report on Privacy and Data Protection: Issues and Challenges, prepared by Professor Greg Tucker, (Monash University, Australia) presents and analyses the results of a survey he conducted in the OECD Member States in order to determine the present situations and trends in privacy and data protection in these countries and the extent to which the OECD Guidelines of 1980 have been followed. The report also reviews selected current issues in privacy and data protection, such as:

- telecommunications and privacy, including subscriber billing systems, telemarketing, caller line identification systems, mobile telephones, telephone cards, transborder data flows and directories
- self-regulation, including a checklist of a set of minimum criteria for an industry/company code of practice and
- transborder data flows, including a review of relevant cases and statistics.

The OECD Guidelines have undoubtedly been influential as a basis for draft and adopted regulation and legislation in non-European countries, for example, Hong Kong, New Zealand and Japan. The report concludes by asking: "what are the means of evaluating the
practical consequences of the endorsement of the Guidelines by companies and other entities?" Its answer is that "it is in the interest of data users and collectors to be able to demonstrate that they observe proper privacy and data protection practices... The evidence of compliance should be concrete and transparent. Claims of adherence to the Guidelines cannot be used as a refuge for lack of protection in this area."

Although published in 1994, the information in the report was collected in 1992.


The US Direct Marketing Association (DMA) has this year released a useful and attractively presented Fair Information Practices Manual, a direct marketer's guide intended to give answers to the most commonly asked questions about implementing corporate fair information policies and complying with the DMA's self-regulatory programs.

1. The manual's first section explains the background to self-regulation.
2. The second section focuses on the development and implementation of corporate fair information policies and actions, covering topics, such as fair information policies, employee training programs and data security.
3. The third section contains the Fair Information Practices Checklist offering companies an opportunity to evaluate their compliance with the fair information principles detailed in DMA's Guidelines for Personal Information Protection.

The pack also includes the DMA's Guidelines on: personal information protection; mailing list practices; marketing by telephone; and ethical business practices.

The "direct" approach to privacy management: the top ten steps

These effective ten steps in complying with good data protection principles have been developed by the US Direct Marketing Association for the benefit of their members. However, in an edited version, they could easily apply to any other user of personal data.

1. Recognise and respond to consumer privacy expectations
2. Know the rules! Legal and self-regulatory responsibilities
3. Develop a corporate fair information policy statement
4. Use the Mail Preference Service and Telephone Preference Service
5. Establish an in-house suppress programme
6. Disclose list rental practices
7. Protect your data - protect your customers. Use: decoys; security programmes; advertising review procedures
8. Stand up and be counted! Communicate your commitment to: customers, media, lawmakers
9. Demand similar standards of your peers
10. Train - train - train!

Swiss Data Protection Law

This book covers a wide field and presents texts in several languages. Its added value is represented particularly by the following:

1. the Swiss Federal Data Protection Act of June, 1992 in German, French, Italian and English
2. the related Swiss Federal Data Protection Ordinance of September, 1993 in German, French, Italian and English
3. A commentary, in German and French, by the authors on the Swiss ordinance
4. A copy of the registration form which must be completed by certain categories of data controllers and submitted to the Swiss Federal Data Protection Commission, with explanatory notes in German and French
5. A copy of the separate registration form which must be completed and submitted to the Swiss Federal Data Protection Commission, in certain circumstances, by data controllers who intend to transfer personal data outside Switzerland, with explanatory notes in German and French

Nearly half of the book is taken by the above sections and represents the best reasons for buying the book.

The rest of the book includes the texts, in French and English, of the Council of Europe Convention on Data Protection (no.108), and the Council of Europe Recommendations on Personal Data used for: Scientific Research and Statistics; Direct Marketing; Employment; Payment and Other Related Purposes.

The book continues with the text of the European Union draft directive on data protection, published in 1992, in German, French, Italian and English.

The final section gives the text of the model contract to ensure equivalent data protection in the context of transborder data flows and the explanatory memorandum, published in 1992 by the Council of Europe, the Commission of the European Union and the International Chamber of Commerce. The final two pages give a list of arbitrators proposed by the Member States of the Council of Europe which includes the principal author of this book, Urs Maurer. He is well qualified for the task as he worked for a time in Switzerland’s Federal Ministry of Justice on the data protection bill. He obtained an LL.M. degree in the USA, is a member of the New York Bar and currently works at the law firm, Bär & Karrer, in Zurich.

Mr. Maurer tells Privacy Laws & Business that his next book, a commentary on the Swiss data protection law, is scheduled to be published in March 1995 by the same publisher. The publisher might consider combining in one volume the material on the Swiss Data Protection Act and Ordinance contained in both the 1994 and the 1995 books and leave the other material for a separate publication. The benefit to the reader would be that the format and print could be larger, making the volume easier to work with. Also, by mid-1995, the 1992 text of the EU draft directive is likely to be superseded.

Datenschutz (Schweizerische Rechtserlasse), by Urs Maurer and Nadine Faruque. Published by Helbing & Lichtenhahn Verlag AG, Freie Strasse 84, CH-4051 Basel, Switzerland. 559 pp. Price S.Fr. 148/DM 170. ISBN 3-7190-1343-X.
Tel: +(41) 64 26 86 86
Fax: +(41) 64 26 86 20
Mr Kevin O'Connor  
Privacy Commissioner  
Human Rights & Equal Opportunity Commission  
Level 2, American Express Building  
388, George Street  
Sydney  
New South Wales 2000  
A U S T R A L I A  
Telephone:  + (61) 2 229 7600  
Fax:  + (61) 2 229 7611

Dr Waltraut Kotchy  
Direktor Buro der Datenschutzkommission und des Datenschutzrates  
Bundeskanzleramt  
Ballhausplatz 1  
1014 Vienna  
A U S T R I A  
Telephone:  + (43) 1 531 15 2528  
Fax:  + (43) 1 531 15 2690

Mr Paul Thomas  
Président  
Commission Consultative de la Protection de la Vie Privée  
Boulevard de Waterloo 115 (postal address)  
Rue de la Regence 61 (office address)  
Brussels 1000  
B E L G I U M  
Telephone:  + (32) 2 542 7200  
Fax:  + (32) 2 542 7212

Mr Bruce Phillips  
Privacy Commissioner for Canada  
112 Kent Street, 14th Floor  
Ottawa, Ontario  
K1A 1H3  
C A N A D A  
Telephone:  + (1) 613 995 2410  
Fax:  + (1) 613 995 1501

Mr Henrik Waaben  
Director  
Registratilsynet  
Christians Brygge 28 4 sal  
1559 Copenhagen V  
D E N M A R K  
Telephone:  + (45) 33 91 16 01  
Fax:  + (45) 33 13 38 43

Dr Jorma Kuopus  
Data Protection Ombudsman  
Post Box 31  
Helsinki 931  
F I N L A N D  
Telephone:  + (358) 0 343 2455  
Fax:  + (358) 0 343 1247

M Jacques Fauvet  
Président  
Commission Nationale de L’Informatique et des Libertés  
21 Rue Saint-Guillaume  
Paris 75007  
F R A N C E  
Telephone:  + (33) 1 4544 4065 or  
+ (33) 1 4548 3939  
Fax:  + (33) 1 4549 0455

Dr Joachim Jacob  
Der Bundesbeauftragte für den Datenschutz  
Postfach 200112  
53131 Bonn  
F E D E R A L  R E P U B L I C  O F  G E R M A N Y  
Telephone:  + (49) 228 819 95 10  
Fax:  + (49) 228 819 95 50

Dr Peter Harris  
The Data Protection Officer  
Advisory and Finance Committee  
States Office  
St Peter Port  
G U E R N S E Y  
Telephone:  + (44) 481 724411  
Fax:  + (44) 481 712520
Mr Thorgeir Orlygsson
Chairman
Icelandic Data Protection Commission
Arnarhvoll
150 Reykjavik
ICELAND
Telephone: + (354) 1 609010
Fax: + (354) 1 27340

Mr Fergus Glavey
Data Protection Commissioner
Block 4, Irish Life Centre
Talbot Street
Dublin 1
IRELAND
Telephone: + (353) 1 8748544
Fax: + (353) 1 8745405

Dr Malcolm Norris
Isle of Man Data Protection Registrar
P O Box 69
Douglas
ISLE OF MAN
Telephone: + (44) 624 661030
Fax: + (44) 624 661088

Ms Sarah Barsela
Registrar of Data Bases
Ministry of Justice
Hillel Street 6
P O Box 2808
Jerusalem 91027
ISRAEL
Telephone: + (972) 2 255 650
Fax: + (972) 2 245 101

Mr Akira Kodaka
Director, Government Information Systems
Planning Division
Management & Co-ordination Agency
Prime Minister's Office
3-1-1 Kasumigaseki
Chiyoda-Ku
Tokyo 100
JAPAN
Telephone: + (81) 3 3581 2078
Fax: + (81) 3 3580 0760

Mrs Val Palmer
Data Protection Registrar
States Greffe
Royal Square
St Helier
JE1 1DD
JERSEY
Telephone: + (44) 534 502014
Fax: + (44) 534 502099

M René Faber
Président
Data Protection Commission
Ministère de la Justice
16 Boulevard Royal
2934
LUXEMBOURG
Telephone: + (352) 478 4552
Fax: + (352) 227 661

Mr Peter Hustinx
President
Registratiekamer
P O Box 3011
2280 GA Rijswijk
THE NETHERLANDS
Telephone: + (31) 70 3 190 190
Fax: + (31) 70 3 940 460

Mr Bruce Slane
Privacy Commissioner
P O Box 466
Auckland
NEW ZEALAND
Telephone: + (64) 9 302 2160
Fax: + (64) 9 302 2305

Mr Georg Apenes
Director General
Datatilsynet
Postboks 8177 Dep 0034
Oslo 1
NORWAY
Mr A Victor Coelho  
President  
Comissão Nacional de Protecção de Dados Informatizados  
Rua de São Bento 148  
1200 Lisboa  
PORTUGAL  
Telephone: + (351) 1 396 6190 or + (351) 1 396 6228  
Fax: + (351) 1 397 6832  

Mr Juan José Martín-Casallo  
Director General  
Agencia de Protección de Datos  
Po de la Castellana 41, 5.a planta  
Madrid 28046  
SPAIN  
Telephone: + (34) 1 308 4702  
Fax: + (34) 1 308 4692  

Ms Anitha Bondestam  
Director General  
Datainspektionen  
Box 8114  
104 20 Stockholm  
SWEDEN  
Telephone: + (46) 8 657 6100  
Fax: + (46) 8 652 8652  

Mr Odilo von Guntern  
Data Protection Commissioner  
Ministry of Justice  
Monbijoustrasse 5  
3003 Berne  
SWITZERLAND  
Telephone: + (41) 31 322 43 95  
Fax: + (41) 31 325 98 96  

Mrs Elizabeth France  
Data Protection Registrar  
Wycliffe House  
Water Lane  
Wilmslow  

Cheshire  
SK9 5AF  
UNITED KINGDOM  
Telephone: + (44) 625 535777 (Enquiries)  
+ (44) 625 535711 (Admin.)  
Fax: + (44) 625 524510  

DIRECTORY OF OTHER DATA PROTECTION AUTHORITIES  

Ms Maureen Tangney  
Acting Executive Member  
Privacy Committee (New South Wales)  
12th Floor  
189 Kent Street  
GPO Box 6  
Sydney  
New South Wales 2000  
AUSTRALIA  
Telephone: + (61) 2 252 3843  
Fax: + (61) 2 252 3842  

Mr David Flaherty  
Information & Privacy Commissioner  
Information & Privacy Commission  
Fourth Floor  
1675 Douglas Street  
Victoria  
British Columbia V8V 1X4  
CANADA  
Telephone: + (1) 604 387 5629  
Fax: + (1) 604 387 1696  

Mr Tom Wright  
Information and Privacy Commissioner/Ontario  
80 Bloor Street West  
Suite 1700  
Toronto  
Ontario M5S 2VI  
CANADA  
Telephone: + (1) 416 326 3333  
Fax: + (1) 416 965 2983  

Mr Paul-André Comeau  
Président  
Commission d’Accès à l’Information de
Quebec
888 Rue Saint-Jean, Bur. 420
Quebec, (Quebec) G1R 5PJ
CANADA
Telephone: + (1) 418 529 7741
Fax: + (1) 418 529 3102

Mr Ulrich Lepper
Chairman, Düsseldorf Kreis
Ministerialrat
Innenministerium des Landes
Nordrhein-Westfalen
Haroldstrasse, 5
Düsseldorf, 4000
FEDERAL REPUBLIC OF GERMANY
Telephone: + (49) 211 871 2251
Fax: + (49) 211 871 3355

Mr Robert J Freeman
Executive Director
Committee on Open Government
New York State Department of State
162 Washington Avenue
Albany
New York 12231
USA
Telephone: + (1) 518 474 2518
Fax: + (1) 518 474 1927

DIRECTORY OF INTERNATIONAL ORGANIZATIONS

Mr Nick Platten
Expert
Commission of the European Communities
Directorate-General 15
200 rue de la Loi (C107 2/20)
Brussels 1040
BELGIUM
Telephone: + (32) 2 295 9862
Fax: + (32) 2 296 1736

Mr George Papapavlou
Directorate-General 13-B
Commission of the European Communities
Bâtiment Jean Monnet
Plateau de Kirchberg
2920
LUXEMBOURG
Telephone: + (352) 4301 4318
Fax: + (352) 4301 2847

Mr Egbert Ausems
Legal Administrator
Public Law Division
Directorate of Legal Affairs
Secretariat General
Council of Europe
P O Box 431 R6
67006 Strasbourg Cedex
FRANCE
Telephone: + (33) 88 41 2000
Fax: + (33) 88 36 7057

Ms Deborah Hurley
Principal Administrator, Science, Technology
& Communications Policy Division
Organization for Economic Cooperation and Development
2 rue André-Pascal
75775 Paris Cedex 16
FRANCE
Telephone: + (33) 1 45 24 82 00
Fax: + (33) 1 45 24 85 00

Mr Karl P Sauvant
Program on Transnational Corporations
UNCTAD
Room E-8006
Palais des Nations
1211 Geneva 10
SWITZERLAND
Telephone: + (41) 22 907 5707
Fax: + (41) 22 917 0194
## European Data Protection Laws

<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Date enacted</th>
<th>Date in force</th>
<th>CE Ratified</th>
<th>Registration/Notification</th>
<th>Manual Records</th>
<th>Legal Person</th>
<th>Data export licence required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Austria</td>
<td>Data Protection Act</td>
<td>18 Oct 78</td>
<td>01 Jan 80</td>
<td>Yes</td>
<td>All data</td>
<td>Yes</td>
<td>Yes</td>
<td>Some data</td>
</tr>
<tr>
<td>Belgium</td>
<td>Law on the Protection of Private Life Regarding the Processing of Personal Data</td>
<td>08 Dec 92</td>
<td>01 Apr 93</td>
<td>Yes</td>
<td>All data</td>
<td>Yes</td>
<td>No</td>
<td>Some data</td>
</tr>
<tr>
<td>Czech and Slovak Republics</td>
<td>The Protection of Personal Data in Information Systems Law</td>
<td>29 Apr 92</td>
<td>01.06.92</td>
<td>No</td>
<td>Some data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Denmark</td>
<td>Private Registers Act</td>
<td>08 Jun 78</td>
<td>01 Jan 79</td>
<td>Yes</td>
<td>Some data</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Finland</td>
<td>Data Protection Act</td>
<td>04 Feb 87</td>
<td>01 Jan 88</td>
<td>Yes</td>
<td>Some data</td>
<td>Yes</td>
<td>No</td>
<td>Some data</td>
</tr>
<tr>
<td>France</td>
<td>Data Processing, Data Files &amp; Individual Liberties Act</td>
<td>06 Jan 78</td>
<td>01 Jan 80</td>
<td>Yes</td>
<td>All data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Germany</td>
<td>Data Protection Act</td>
<td>27 Jan 77</td>
<td>01 Jan 79</td>
<td>Yes</td>
<td>Some data</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Guernsey</td>
<td>Data Protection Act</td>
<td>30 Jul 86</td>
<td>11 Nov 87</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Hungary</td>
<td>Protection of Personal Data and Disclosure of Data of Public Interest Act</td>
<td>27 Oct 92</td>
<td>01 May 93</td>
<td>No</td>
<td>Some data</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Iceland</td>
<td>Systematic Recording of Personal Data Act</td>
<td>05 Jun 81</td>
<td>01 Jan 93</td>
<td>Yes</td>
<td>All data</td>
<td>Yes</td>
<td>Yes</td>
<td>All data</td>
</tr>
<tr>
<td>Ireland</td>
<td>Data Protection Act</td>
<td>13 Jul 88</td>
<td>19 Apr 89</td>
<td>Yes</td>
<td>Some data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Isle of Man</td>
<td>Data Protection Act</td>
<td>16 Jul 86</td>
<td>17 Oct 90</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Jersey</td>
<td>Data Protection Act</td>
<td>30 Apr 87</td>
<td>11 Nov 87</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>The Use of Name Linked Data in Computer Processing Act</td>
<td>31 Mar 79</td>
<td>01 Oct 79</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Netherlands</td>
<td>Data Protection Act</td>
<td>28 Dec 88</td>
<td>01 Jul 90</td>
<td>Yes</td>
<td>Some data</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Norway</td>
<td>Personal Data Registers Act</td>
<td>09 Jun 78</td>
<td>01 Jan 80</td>
<td>Yes</td>
<td>Some data</td>
<td>Yes</td>
<td>Yes</td>
<td>Some data</td>
</tr>
<tr>
<td>Portugal</td>
<td>Protection of Personal Data Act</td>
<td>29 Apr 91</td>
<td>04 May 91</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>All data</td>
</tr>
<tr>
<td>Spain</td>
<td>Law on the Regulation of the Automated Processing of Personal Data</td>
<td>29 Oct 92</td>
<td>01 Feb 93</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>Some data</td>
</tr>
<tr>
<td>Sweden</td>
<td>Data Act</td>
<td>13 May 73</td>
<td>01 Jul 74</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>Some data</td>
</tr>
</tbody>
</table>
### European Data Protection Laws (Continued)

<table>
<thead>
<tr>
<th>Country</th>
<th>Legislation</th>
<th>Date enacted</th>
<th>Date in force</th>
<th>CE Ratified [see note]</th>
<th>Registration/Notification</th>
<th>Manual Records</th>
<th>Legal Person</th>
<th>Data export licence required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switzerland</td>
<td>Data Protection Act</td>
<td>19 Jun 92</td>
<td>01 Jul 93</td>
<td>No</td>
<td>Some data</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>UK</td>
<td>Data Protection Act</td>
<td>12 Jul 84</td>
<td>11 Nov 87</td>
<td>Yes</td>
<td>All data</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Notes**
- This table is intended to provide a summary of certain aspects of each law. It is not intended to be comprehensive or to render legal or other professional advice. The table is based on information available at 13th December 1994.
- All European data protection laws, subject to various exemptions, cover automated data in both public and private sectors relating to physical persons, give data subjects a right of access to records on themselves, together with a right of correction or a right to file a note of disagreement. All give powers to a Data Protection Authority to impose orders restricting the export of data in certain circumstances, and all contain provision for imposing penalties on those who breach the law.
- "CE" means the Council of Europe's Convention for the protection of Individuals with regard to the Automatic Processing of Personal Data (in force October 1985).

### European Data Protection Bills

<table>
<thead>
<tr>
<th>Country</th>
<th>Title of Bill</th>
<th>Date intro. to legislature</th>
<th>Est. date in force</th>
<th>CE Ratified [see note]</th>
<th>Registration/Notification</th>
<th>Manual Records</th>
<th>Legal Person</th>
<th>Data export licence required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greece</td>
<td>Bill on the Protection of the Individual with Regard to the Processing of Personal Data</td>
<td>Nov 87</td>
<td>N/A</td>
<td>No</td>
<td>All data</td>
<td>Yes</td>
<td>No</td>
<td>Some data</td>
</tr>
<tr>
<td>Italy</td>
<td>Bill on the Protection of Individuals in relation to the Automatic Processing of Personal Data</td>
<td>01 Sept 92</td>
<td>N/A</td>
<td>No</td>
<td>Some data</td>
<td>Yes</td>
<td>Yes</td>
<td>Some data</td>
</tr>
</tbody>
</table>

**Notes**
- This table is intended to provide a summary of certain aspects of each bill. It is not intended to be comprehensive or to render legal or other professional advice.
- Several of these bills have been redrafted at various times. This table is based on information available as at 13th December 1994 and is believed correct as at that date.
- All European data protection bills, subject to various exemptions, cover automated data in both public and private sectors relating to physical persons, give data subjects a right of access to records on themselves, together with a right of correction or a right to file a note of disagreement. All give powers to a Data Protection Authority to impose orders restricting the export of data in certain circumstances, and all contain provision for imposing penalties on those who breach the law.
- "CE" means the Council of Europe's Convention for the protection of Individuals with regard to the Automatic Processing of Personal Data (in force October 1985).
- "N/A" means information not available.