THE NETHERLANDS DATA PROTECTION BILL

The Data Protection Bill's Current Status

The Data Protection Bill was accepted by the Lower House of the Dutch parliament in September 1987 and was then passed to the Upper House. The Upper House does not have the power to amend the bill and can only say yes or no. The bill is currently at the committee stage where questions are put to the government which will be followed by a general debate. I expect this debate will take place in the course of November or December and that the bill will be passed by parliament around the end of the year.

The Background to the Bill

In order to understand this legislation, it is important to understand its history. In 1971 there was a periodical census in the Netherlands, and a large proportion of citizens refused to co-operate. Some individuals were brought to court on criminal charges. Finally the case was dropped, but it created a big political row.

Since this refusal to cooperate with the census was obviously related to privacy worries, the government promised to set up a Royal Commission (the Koopmans Commission), to study the problem. The Royal Commission issued its report in 1976. It contained a draft bill and commentary following the Swedish model with a licensing system.

In 1975, just a year before that, the government, expecting that it might take some time to collect comments, and that another approach might have to be taken, decided to lay down a policy of self-regulation for central government files. The rationale was that it was not necessary to wait for formal legislation to be passed by parliament. Instead the government could introduce self-regulation in the form of provisional measures for the protection of privacy. As a result, the government issued guidelines saying that no personal data file, no automated file should be kept in the central administration without complying with a published set of rules laid down by the controlling authority.

These guidelines are still in effect and still working and there are now about 200 or 250 different regulations for automated personal data files in the central government. These regulations are not perfect. They are provisional. But they have led the way in establishing clear practice in the direction of data protection legislation. The example was followed by local government, provincial government and municipal government, and by several sectors of private industry. So self-regulation in data protection is a well-established practice in the Netherlands.

In addition, under a general heading of civil law, criminal law, and administrative law, we've had cases, and a growing number of cases, in which courts have given their decision on privacy matters. So on top of self-regulation practice we have had, in the absence of formal legislation, many precedents dealing with the subject.

In 1981 finally, the government submitted the first data protection bill. Not the current one, but the one which was based on the report submitted 5 years before, which followed the Swedish approach.

It met severe criticism, not only in parliament but also outside parliament. It was felt to be too bureaucratic and too complicated. In addition, it was felt that its scope was too limited because it dealt with only automated files. Most people felt that with a subject like this the regulations should not be limited to automated files because it is a general problem, which should be addressed in a general way.

Finally, we had a change of constitution. The Dutch constitution was revised and a new text promulgated in 1983. It contained a general provision on the right to respect privacy and in addition laid down an obligation to legislate on the protection of privacy regarding personal data. This bill is meant to give effect to the constitutional provision, and is intended to give effect to the Council of Europe Convention as well.

The Data Protection Bill

1. Scope

We have deliberately tried to come up with a regulation which is as simple as possible. The scope of the bill is much wider than the original.

* This bill covers automated and non-automated files as well. In the latter case, a file has been defined in such a way that it covers data which is systematically accessible and structured.

* It is concerned with physical persons only and the definition of personal data follows that of the Council of Europe quite closely.

* It relates to the public and the private sectors, and in substance it makes little difference. The main provisions apply to both sectors.

* It contains some exemptions - it does not apply for instance to personal data which by its nature is intended for personal or domestic use. Examples are the typical private notebook in computer form, and things which by their nature happen at home. This exemption does not apply to a businessman working at home. This is an example of data protection meeting privacy protection. In this instance we have chosen privacy protection rather than data protection.

We have excluded data files which are intended solely for use in the supply of information to the public by the press. This provision enables a reconciliation between freedom of information and privacy principles. There, it is freedom of information saying stop to data protection.

We have exempted the police and the secret services - not completely but there will be a special Act in the former case, and there is already one in the latter case, dealing with privacy protection in these fields.

2. Material Standards

The bill addresses the controller along the lines of the Council of Europe Convention and it deals with the processor who is more or less the computer bureau in the UK legislation. The Act contains material standards which are directly applicable - they may be applied directly or they may be enforced - applying to all these personal data files.

The "iron triangle" of data protection principles is reflected in the text:

Firstly, the purpose should be specific, specified and legitimate. In the case of a file set up by a government agency, it should be necessary for the task of this particular agency.

Secondly, the file may contain only data which is in accordance with that purpose. The data should be obtained fairly and legitimately; and in the case of a government agency the data should be necessary for the purpose of the file. There should be necessary measures to ensure accuracy and completeness. All this has been written down in very short statements of principle.

Thirdly, data may be used only in a way compatible with the purpose of the file.

3. Sensitive Data

The bill does not go into details as far as sensitive data is concerned - further rules will be laid down within a year. Three years later - as stated in the bill - there should be a change in the law with provisions dealing with these sensitive matters. Frankly, we did not manage to work out these rules before introducing the bill and this is just a procedure to agree on a solution.

4. Data Security

There is a section stating the responsibility of the controller in terms of security. He should take the necessary technical and organisational measures to maintain security, according to the technical possibilities, the nature of the file and so on.

5. Transfer of Data to a Third Party

There are provisions in part 3 of the bill dealing with the communication of information to third parties. The basic rule is that the transfer of data to a third party may take place only if it follows from the purpose. In addition to that, such a transfer may take place under a statutory requirement, typically taxes and social security, and with the consent of the data subject. This consent should be specific and in writing after the data subject has been given proper information.

For special cases we have some provisions for statistics, emergencies etc. Section 13 deals with information bureaux, the typical case where the purpose of the file is communication of data to third parties. Section 14 deals with the transfer of names and addresses which may be communicated in

certain situations but not if the data subject has objected.

6. Codes of Conduct and Registration

These provisions are very general. We wanted to differentiate according to sectors because these rules have to be applied to the specific problems of each sector. A way to do that is to allow for self-regulation, which is envisaged on two levels in this bill. If the Data Protection Act is seen as the top level, then there is self-regulation on both the middle level, the sector level, and at the base, the data processing file level.

6.1 The Sector Level

On the middle level there is a chapter (Part 4) dealing with codes of conduct. Codes of conduct may be developed without the law saying so. But according to section 15 the code of conduct may be submitted for approval to our data protection authority, the Registration Chamber. Then the authority will have to check:

* whether the organisations submitting the code are sufficiently representative for the sector to which the code applies.

* that the code has been drawn up with due care and with adequate consultation with other interested organisations. So if, for example, a social research association submits a perfect code but has given no-one else an opportunity to comment, then approval will not be possible. It is a mechanism to promote a process of bargaining.

* that the code is in conformity with the Data Protection Act, and fulfills reasonable requirements for the protection of the privacy of data subjects.

A code of conduct approved by the Registration Chamber is not legally binding but in practice it will have considerable authority. The more care given to the preparation and procedure according to which it is approved, the more authority it will have. So a controller or institution which wants to forget about this code might run into problems.

The approval of the Registration Chamber is valid for only 5 years. After this time the code will have to be re-submitted for approval if the organisation would like to work within its approved framework.

In section 16 there is an interesting sanction. If a sector does not develop a code of conduct where the Registration Chamber thinks it necessary, or where a code has been developed but is not enforced in practice, then the government may step in and lay down binding rules. This is possible only after 3 years to give organisations time to develop their own codes of conduct. The explicit purpose of this provision is to give leverage to promote self-regulation.

6.2 The File Level

The bill also covers self-regulation on the base level, that of the

data processing file. In parts 5 and 6 of the bill there is a distinction between the public and the private sectors.

In the public sector, including education, health care and the like there is a duty to lay down regulations, formal rules, the subjects of which are spelled out in the law - purpose, content, transfer to third parties etc. These rules should be made public, and notification given to the Registration Chamber. These rules are binding on the controller, an outside data processing bureau and all others involved in the file. All have to comply with these regulations. Clearly, it is dangerous to lay down rules and forget about them because that would lead to illegal conduct. It is possible to change the regulations but of course these regulations have to be in conformity with the law, they have to be published, and new notifications sent to the Registration Chamber.

In the private sector there is a duty to give notification with a formal form which, in the way it has been worked out, is very close to the formal regulations for the public sector - only it will be much simpler. It will deal with the same subjects, (purpose, content, use etc.) and the notification will be binding on the controller and his entire organisation. Once he has issued his notification to the Registration Chamber it is binding. It is public, so interested parties may go to court and ask for enforcement.

6.3 Exceptions

There are interesting exceptions for both public and private sectors because we felt that a law with such a wide scope, covering all automated and manual personal data, could never impose a duty of regulation and notification to the fullest extent. So we adopted a rule of thumb that the obvious does not have to be regulated, or notified. That is why there is an exception for these obvious cases like staffing and payroll systems, accounting systems, subscription records, membership and things like that. There will be an administrative order - executive regulation - giving the exact description of the standard cases which do not have to be notified.

The policy idea is that about 80% of the files will be covered by an exception so the Registration Chamber will be able to concentrate on the exceptional rather than the obvious cases. Again, the controller has his choice - he can choose to be covered by the standard. Alternatively, he can say that he has special reasons for doing it in a different way. In that case he has to notify the Registration Chamber - that is implicit self-regulation. The purpose is obvious - to limit bureaucracy and to concentrate limited funds on high priority tasks.

7. Rights of Information and Correction

The provisions on the rights of information and correction impose a duty on the controller to notify a person that data on him has been entered into a file for the first time - but again there is an exception that the obvious does not have to be reported. If a data subject is aware of the existence of a file, then notification is not necessary:

* If I take a subscription to a newspaper then the newspaper does not have to tell me that I am on the subscribers' list.

* It is possible, for instance in banking and credit institutions, to give advance information that asking for credit will lead to credit reporting at a certain credit information organization.

The right to information includes information stored on the source of the data, and the communication of the data to third parties. Third parties in the Netherlands bill includes other legal persons. Once again, the controller does not have to state the obvious - if every month or every year there is communication of salary data to the tax authorities, or wages are being paid, he does not have to give such information to the data subject.

His duty is greater when data of a very sensitive nature is involved. When a medical file is involved, the controller has a much wider duty of care than when only names and addresses are involved, provided the addresses do not relate to a group which has a very sensitive background.

8. Enforcement

8.1 Penal Sanctions

There are only a very few penal sanctions to be found in this bill. Practically the only duty subject to penal sanction is to notify the existence of a file and to lay down regulations. Having a black list would be illegal and would lead to penal sanction.

8.2 Informal and Civil Sanctions

Aside from that, it is purely a matter of informal and civil sanctions. A data subject may go to the Registration Chamber and ask for an investigation. The Chamber has full powers to investigate the case. It may then recommend a certain course of action to the data protection controller and it may make this recommendation public. It will give the outcome of the investigation both to the controller and to the complainant. This has been done in a deliberate effort to trigger off a civil case if the controller does not follow up the recommendation. But the Registration Chamber does not have the power to go to court. It may use informal sanctions to bring pressure - like going to the press - but it does not have the power to go to court. Instead we have included sections 9 and 10 in the Act which make it easier than usual for interested parties to go to court.

8.3 Damages

Section 9 deals with liability. First of all on top of normal tort liability, it allows for immaterial damage. In section 9.3 there is a provision on strict liability for a controller of the file. The controller will be held liable for any damages material or immaterial resulting from acts or ommissions which are contrary to the rules of the Act or contrary to the rules in the regulations or the notification requirement. The liability of the controller even covers computer faults, and any actions or omissions at a computer bureau. A processor or computer bureau shall be liable for any loss or damage resulting from his actions.

8.4 Rights for Legal Persons

According to section 10, not only the data subject himself but also legal persons like consumer unions, labour unions, and civil liberty groups may act to protect their interests. This is a mechanism growing in importance in the Netherlands and we expect it to work well in the area of data protection.

9. International Transfers of Data

Sections 47, 48 and 49 deal with international aspects. In principle, the Dutch Data Protection Act will apply to everything that happens on Dutch territory.

In addition, the law will apply to a personal data file not located in the Netherlands - but kept by a controller established in the Netherlands. If a Dutch insurance company has its data in Germany or the UK, Dutch law would apply to the controller and to the data. It should make no difference whether the data is being stored in UK, Germany or wherever around the world. In the above examples, German and UK law may also be applicable. In Section 47.2 the Minister of Justice, having consulted the Registration Chamber, may give an exemption in a specific case. That is just a way to accommodate possible conflicts of law.

Another case of a Minister of Justice exemption, covered by section 48, is where a controller outside the Netherlands, say the USA, Australia or South America may have his data in the Netherlands because a computer is located there as part of a worldwide network. Then, it would not be very practical to apply Dutch law, provided that there is proper security in the Netherlands bureau and provided that there are adequate safeguards for the privacy of the data subject. The Data Protection Bill therefore ensures public order, as the Netherlands does not want to be a data haven.

We do not have a provision laying down the requirements for a license on transborder data flows. There is only in section 49 the possibility of an emergency brake if a file is set up in another country in an effort to circumvent Dutch law. If such a transfer of data has serious adverse effect on the privacy of the persons concerned, then any communication back and forth to that file may be banned under criminal sanctions.

10. Summary

In short, the bill consists of general provisions and self-regulation but the sword of Damocles in terms of enforcement. No criminal cases because the courts are blocked. In terms of crime, data protection is relatively unimportant. In civil cases, the outcome may be heavy sanctions. In theory the court may say, stop the operation or change the system. The idea is that the controller will look ahead and build in a certain margin of data protection and work out what is really necessary; this is again a kind of self-regulation.

This is an edited version of a paper given by Mr Peter Hustinx, Legal Advisor on Public Law, the Netherlands' Ministry of Justice, the Hague at the Privacy Laws & Business Conference on October 19th in London.