

EUROPEAN PARLIAMENT

# Working Documents

1981 - 1982

---

12 October 1981

DOCUMENT 1-548/81

## Second Report

drawn up on behalf of the Legal Affairs Committee

**on the protection of the rights of the individual in the face of technical  
developments in data processing**

**Rapporteur: Mr H. SIEGLERSCHMIDT**



At its sitting of 17 April 1980, the European Parliament referred to the Legal Affairs Committee a motion for a resolution (Doc. 1-103/80) tabled by Mrs Roudy and others pursuant to Rule 25 of the Rules of Procedure on the protection of private life.

At its meeting of 29 April 1980 the Legal Affairs Committee appointed Mr Sieglerschmidt rapporteur.

On 17 April 1980 the European Parliament also referred to the Legal Affairs Committee a motion for a resolution (Doc. 1-116/80) tabled by Mr Glinne and others on behalf of the Socialist Group pursuant to Rule 25 of the Rules of Procedure on the protection of individuals against data processing.

At its meeting of 4 June 1980, having regard to the close connection between the two motions for resolutions, the Legal Affairs Committee appointed Mr Sieglerschmidt rapporteur for this motion for a resolution also and instructed him to deal with both motions for resolutions in a second report on the protection of the rights of the individual in the face of technical developments in data processing<sup>1</sup>.

The Legal Affairs Committee examined the draft report drawn up by Mr Sieglerschmidt at its meetings of 25 and 26 June 1981 and 22 and 23 September 1981 and adopted the motion for a resolution unanimously at the latter meeting.

Present: Mr Ferri, chairman; Mr Turner and Mr Chambeiron, vice-chairmen; Mr Sieglerschmidt, rapporteur; Mrs Cinciari Rodano, Mr Dalziel, Mr d'Angelosante, Mrs van den Heuvel (deputizing for Mr Blaskovitis), Mr Janssen van Raay, Mr Megahy, Mr Peters (deputizing for Mr Vetter), Sir James Scott-Hopkins (deputizing for Mr Prout), Mr Tyrrell and Mrs Vayssade (deputizing for Mrs Théobald-Paoli).

---

<sup>1</sup> The first report, by Mr Bayerl (Doc. 100/79), was adopted by the Legal Affairs Committee on 6 April 1979 (resolution of the European Parliament of 8 May 1979, OJ N° C 140, 5.6.1979, p. 34)

# C O N T E N T S

	<u>Page</u>
A. MOTION FOR A RESOLUTION .....	5
B. EXPLANATORY STATEMENT .....	10
I. Introduction .....	10
II. Review of the present situation with regard to data- protection legislation and work in progress .....	11
(a) Commission of the European Communities .....	11
(b) Council of Europe .....	12
(c) Organization for Economic Cooperation and Development (OECD) .....	15
(d) Member States of the European Communities .....	17
(e) Other member countries of the Council of Europe.....	23
(f) OECD countries .....	26
III. Questions to be decided .....	28
(a) Compatibility of the provisions of the Council of Europe's convention with the European Parliament's demands .....	28
(b) Need for Community law .....	30
(c) Accession of the European Community to the Council of Europe's convention .....	32
IV. Conclusions .....	33
Annex I: Motion for a resolution by the Socialist Group on the protection of individuals against data processing of 17 April 1980 (Doc. 1-116/80) .....	35
Annex II: Motion for a resolution by Mrs Roudy and others on the protection of private life of 16.4.1980 (Doc.1-103/80) 36	36
Annex III: Text of the European Convention for the protection of individuals with regard to automatic processing of personal data .....	37
Annex IV: Text of the OECD guidelines on privacy protection and transborder data flows.....	46

A

The Legal Affairs Committee hereby submits to the European Parliament the following motion for a resolution together with explanatory statement :

MOTION FOR A RESOLUTION

on the protection of the rights of the individual in the face of technical developments in data processing

The European Parliament

- having regard to its debates of 8 July 1974<sup>1</sup> and 21 February 1975<sup>2</sup>
- having regard to its resolution<sup>3</sup> of 8 April 1976 in which it :  
instructed its Legal Affairs Committee to report to it on Community activities to be undertaken or continued with a view to safeguarding the rights of the individual in the face of developing technical progress in the field of automatic data processing, and

invited the Commission of the European Communities to take steps to ensure that the collection of data and information intended as a basis for the drafting of Community legislation in this field was brought to a conclusion under its authority,

- having regard to the joint declaration by the European Parliament, the Council and Commission on respect for fundamental rights<sup>4</sup>,
- having regard to its resolution<sup>5</sup> of 8 May 1979 in which it called upon the Commission to prepare a proposal for a directive on the harmonization of legislation on data protection to provide the citizens of the Community with the maximum protection, and

urged strongly the Commission and the Council when preparing legislation on data protection to take the fullest account of the recommendations appended to that resolution of which they were an integral part,

---

<sup>1</sup>OJ Debates No. 179 page 54 et seq.

<sup>2</sup>OJ Debates No. 186 page 254

<sup>3</sup>OJ No. C 100, 3.5.1976, page 27

<sup>4</sup>OJ No. C 103, 27.4.1977, page 1

<sup>5</sup>Doc. 100/79

recommended the Member States to coordinate their efforts in all the international forums where these questions are discussed and once the Council of Europe Convention had been signed to work for the accession to that convention of the greatest possible number of third countries, subject to reciprocity,

- having regard to its debates of 24 September 1979<sup>1</sup>
  - whereas according to Article 17 of the International Covenant on civil and political rights (no one shall be subject to arbitrary or unlawful interference with his private life) everyone is entitled to protection under the law against such interference or encroachment,
  - having regard to the European Convention for the Protection of Human Rights and Fundamental Freedoms (principle of respect for privacy),
  - having regard to the resolution of the Organization for Economic Cooperation and Development (OECD) of 22 July 1979,
  - having regard to the motion for a resolution tabled by Mrs Roudy and others (Doc. 1-103/80),
  - having regard to the motion for a resolution tabled by Mr Glinne and others on behalf of the Socialist Group (Doc. 1-116/80),
  - having regard to the report of the Legal Affairs Committee (Doc. 100/79),
  - having regard to the second report of the Legal Affairs Committee (Doc. 1-548/81),
1. Welcomes the resolution of the Committee of Ministers of the Council of Europe of 18 September 1980 approving this Convention for the protection of individuals with regard to automatic processing of personal data;
  2. Is however concerned that it is not clear when all the Member States of the Community will finally have signed and ratified this European Convention;
  3. Considers that rules on the protection of personal data are also feasible and necessary for the Community and that the European Convention should be adapted accordingly;

<sup>1</sup> OJ Debates N° 245, page 19 et seq.

4. Takes the view that modern technology may pose serious threats to the rights of the individual and in particular to the right to respect for privacy;
5. Notes that a number of Community countries do not yet have laws protecting the citizen from the misuse of data files and data processing or that such laws where they exist may differ in the level of protection, the procedural principles or the rules they contain;
6. Refers to Article 100 of the EEC Treaty providing for the approximation of such provisions laid down by law, regulation or administrative action in the Member States as directly affect the establishment or functioning of the Common Market;
7. Is of the opinion that the corresponding directive when issued should not only approximate but progress beyond the relevant provisions of the Member States;
8. Considers that the use of data processing and transmission techniques particularly in the light of rapid technological change, demands periodic review at a Community level;
9. Takes the view that the European Community as a Community set up for economic and commercial purposes must have power to eliminate related problems and protect the citizens of Europe by means of general, uniform and effective provisions in the field of data protection;
10. Considers that data transmission in general should be placed on a legal footing and not be determined merely by technical considerations;
11. Considers that thought should be given to investigating the possibility and desirability of expressly incorporating the right to the protection of personal data as a human right or fundamental freedom in the text of the European Convention for the protection of Human Rights and Fundamental Freedoms in the form of a sixth protocol;
12. Calls upon Member States to comply with the Commission Recommendation of 29 July 1981 on the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data, namely to sign it before the end of 1981 and to ratify it before the end of 1982, and further to give legal effect to the provisions thereof;
13. Calls upon the Commission to undertake regular consultation with the Consultative Committee of the said Convention on personal data and to review its work;
14. Believes that the European Community should in due course accede to the abovementioned convention in its own right;

15. Considers nevertheless that there remains an urgent need for a Community directive with special care being taken to ensure that
- the same level of protection from such technologies is afforded in both the private and the public sector and that such protection shall extend to all data of a personal nature irrespective of national borders,
  - the directive shall include an obligation to notify the person concerned who shall be entitled to have access to, and to correct, information concerning him;
  - liability for damage caused shall be introduced,
  - the operation of data banks shall be subject to obligatory notification and approval on a national basis;
16. Considers it essential that a Community body should be set up with the sole task of defining and supervising compliance with conditions for the transmission of data across frontiers;
17. Instructs its President to forward this resolution to the Council, the Commission, the Court of Justice and the governments and parliaments of the Member States, the Assembly and the Committee of Ministers of the Council of Europe, the Council of the Organization for Economic Cooperation and Development and the national bodies responsible for supervising the application of general or specific legal provisions on the protection of freedoms.



### Prefatory note

This Second Report on behalf of the Legal Affairs Committee on the protection of the rights of the individual in the face of technical developments in data processing is a sequel to the First Report<sup>1</sup> drawn up by Mr Alfons Bayerl in 1979.

In drawing up this second report the rapporteur's intention is not to present a totally new and different report, but rather to take into account subsequent developments in the data-processing field - whether in the form of international agreements or other provisions or more recent legislation in the Member States or third countries - in other words, to update the Bayerl report.

---

<sup>1</sup> Doc. 100/79

B  
EXPLANATORY STATEMENT

I. Introduction

1. In May 1979 the First Report on the protection of the rights of the individual in the face of technical developments in data processing was presented to the European Parliament by its rapporteur, Mr BAYERL, and the motion for a resolution was adopted unanimously<sup>1</sup>.

Important points in the resolution were the request to the Commission to prepare a proposal for a directive on the harmonization of legislation on data protection to provide citizens of the Community with the maximum protection and the recommendation to the Member States to coordinate their efforts in all the international forums where these questions are discussed and to work for the accession to the Council of Europe convention of the greatest possible number of countries.

2. On 24 September 1979 a debate on data protection<sup>2</sup> was held in the European Parliament on the basis of an oral question by Mr van Aerssen and Mr Alber on behalf of the Group of the European People's Party. In that debate speakers from all the groups voiced their conviction that a Community directive was as necessary as ever. Particular attention was drawn to the need for Community legislation on transborder data flows and to three principles to be observed in the drafting of the directive: it must preserve a balance of information between the Member States, ensure the legality of the processing of data, and be formulated in legally unambiguous terms<sup>3</sup>. It was also stressed that the directive must provide the highest level of protection<sup>4</sup>.

The Commissioner, Mr Natali, affirmed that the Commission was aware of the importance of this subject, but wanted to wait until the text of the Council of Europe convention was available before submitting proposals for a directive<sup>5</sup>.

---

<sup>1</sup> Annex I, Doc. 100/79

<sup>2</sup> OJ Debates No. 245, p.19 et seq.

<sup>3</sup> *ibid.* loc. cit.

<sup>4</sup> *ibid.* p.22

<sup>5</sup> *ibid.* p.20

3. In response to further written questions in November<sup>1</sup> and December<sup>2</sup> 1979 and in April<sup>3</sup>, June<sup>4</sup> and July<sup>5</sup> 1980, concerning further Community work in the data-protection field, Members of the Commission referred again to the need to await the outcome of the Council of Europe's work. In the answer to written question to the Council of Ministers July 1980<sup>6</sup> reference was made to the studies being carried out under the Commission's auspices.

In April 1980 the Socialist Group of the European Parliament tabled a motion for a resolution on 'the protection of individuals against data processing'<sup>7</sup>.

The motion for a resolution by Mrs Roudy and others on 'the protection of private life'<sup>8</sup> contained similar observations.

On 4 June 1980 the rapporteur of the Legal Affairs Committee, to which these resolutions had been referred, was asked to draw up a report on the subject<sup>9</sup>.

## II. Review of the present situation with regard to data-protection legislation and work in progress

### (a) Commission of the European Communities

4. At the beginning of 1978 the Commission set up a Group of Experts on Data Processing and the Protection of Privacy, which decided at its constituent meeting to await finalization of the preliminary draft convention of the Council of Europe before deciding what position the Community should adopt<sup>10</sup>.

At its subsequent meeting it decided to carry out a substantial long-term research project covering the following points:

- nature and scope of transborder data-flows
- legal structure of data-protection bodies
- the problem of legal and natural persons

---

<sup>1</sup> OJ No. C 156, 25.6.1980, p.19

<sup>2</sup> OJ No. C 160, 30.6.1980, pp 11-12

<sup>3</sup> OJ Nos. C 178, 16.7.1980, pp 58-59 and C 198 of 4.8.1980, pp 35-36

<sup>4</sup> OJ No. C 255 of 2.10.1980, p.16

<sup>5</sup> OJ No. C 245, 22.9.1980, pp 15-16

<sup>6</sup> OJ No. C 283, 3.11.1980, p.20

<sup>7</sup> Annex I, Doc. 1-116/80

<sup>8</sup> Annex II, Doc. 1-103/80

<sup>9</sup> cf PE 65.865, p.9, (c)

<sup>10</sup> Commission Doc. III/268/78

- costs connected with international rules on personal data
- technical aspects of right of access
- control, scrutiny and the implications for data protection of stricter rules on security.

5. In November 1979 the group of experts discussed the Community's position on the Council of Europe's draft convention which had meanwhile become available. The majority of the participants considered that, in view of the possibility of the Community acceding to the convention, there was no urgent need for a Community directive to be adopted in this field, but they were aware that the Community's accession to the convention would create a number of difficulties<sup>1</sup>. It was generally believed, however, that the 'hard core' of the draft convention offered a sound basis for the Community's own work.

6. In May 1980 the research institutes commissioned to carry out the study referred to above presented their report, which ran to several volumes<sup>2</sup>. It was expected that this work would continue for the rest of the current four-year programme.

#### (b) Council of Europe

6a. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms contains a provision in general terms guaranteeing everyone the right to respect for his private life. In the light of rapid technical advances being made in the field of data protection it seems worthwhile considering whether Article 8 should not be buttressed by including expressly in the text of the European Convention on Human Rights the right to the protection of personal data as a human right or fundamental freedom. The Council of Europe's efforts to extend the list of fundamental freedoms protected by the European Convention on Human Rights have produced a number of preliminary drafts for a sixth protocol to the Convention. The Parliamentary Assembly of the Council of Europe has, in conformity with the preliminary draft of a sixth protocol to the European Convention on Human Rights drawn up by the International Union of Lawyers, recommended the incorporation into the Convention of, inter alia, a right to the protection of data<sup>3</sup>.

---

<sup>1</sup> cf Council of Europe Doc. 4472, p.6

<sup>2</sup> Final report of the EEC research project 'Data protection and security' prepared by the GMD, IRIA and NCC research institutes for the Commission, St Augustin 1980

<sup>3</sup> See Recommendation 890 (1980) of 1.2.1980

7. After preliminary work, begun as far back as 1968, a committee of experts set up by the European Committee on Legal Cooperation (CDCJ) submitted the draft of a 'Convention for the protection of individuals with regard to automatic processing of personal data'<sup>1</sup>. This draft was finalized by the CDCJ at its meeting of 27.6.1980 and forwarded to the Committee of Ministers.

8. On 10 February 1980 the Parliamentary Assembly of the Council of Europe, after considering a report drawn up by Mr Holst on data processing and the protection of human rights<sup>2</sup>, also adopted Resolution 721 (1980) on 'Data processing and the rights of the individual'<sup>3</sup>. In this resolution the European Parliament was urged to keep a close watch on the application of the principles of the future convention and thus assist, within the framework of the Community's activity, in establishing the data protection called for. In addition, the parliaments of those countries in which there were still no data-protection provisions were urged to introduce legislation of their own, taking into account the principles defined by the Council of Europe.

In this connection it should be pointed out that one reason why the finalization of the draft convention was speeded up was to enable the Community to accede to the Convention once the Member States had done so.

There appears to be a good chance of this happening from the broad measure of agreement on the draft convention expressed in the European Committee on Legal Cooperation by the member countries of the Council of Europe, which include all the Member States of the Community. Of the 21 Member countries only Malta voted against the draft; the Federal Republic of Germany abstained because there were some doubts about the compatibility of the draft convention with the data-protection law of one of the 'Länder'. These doubts have since been removed.

9. The draft convention was approved on 18 September 1980 by the Committee of Ministers<sup>4</sup>, which will now fix the date from which the convention will be open for signing by non-member countries as well as by member countries of the Council of Europe.

The Convention was signed on 28 January 1981 by Austria, Denmark, the Federal Republic of Germany, France, Luxembourg, Sweden and Turkey. Subsequently, Norway and the United Kingdom have also signed the Convention.

#### Contents of the Convention

10. As the title indicates (Convention for the protection of individuals with regard to automatic processing of personal data), the convention is concerned only with personal data in the field of automated data processing.

<sup>1</sup> Council of Europe Doc. CJ-PD(79) - Miset

<sup>2</sup> Council of Europe Doc. 4472

<sup>3</sup> PE 63.693

<sup>4</sup> Official text of the Convention cf Annex III CDCJ (28), Add.1

Chapter I contains general provisions defining the object, purpose and scope of the convention. The convention covers data banks in the public and private sectors. However, according to Article 3(2c) the signatory states are free to apply it to manual processing. Another way in which the scope of the convention may be optionally extended is for the signatory states to grant data-protection rights to groups of persons, associations, foundations, companies, corporations or any other bodies (Art.3(2b)). In Article 3(2a), on the other hand, it is left to the signatory states, if they wish, to exclude certain categories of data from the scope of the provisions.

Chapter II (Articles 4-11) sets out the basic principles governing data protection, which include the fair and lawful collection of data, the relevance of the data stored and the way they are used to the purpose for which they are intended, restrictions on the storing of particular data, the updating of the data and prohibition on the storing of sensitive data such as political opinions. Furthermore, the data subject has the right to obtain information about the nature of the data concerning him from the agency officially responsible for him and to demand that incorrect data be corrected. Exceptions are allowed only in the interests of public safety, preventing criminal acts, protecting the fiscal interests of the State or protecting the data subject or third persons.

Chapter III (Article 12) refers to transborder data transmission. In Article 12(2) it is emphasized that the signatories to the convention are not entitled to make the transborder transmission of personal data between themselves subject to authorization solely for the purpose of protecting privacy. Article 12(3) allows any signatory to adopt provisions restricting the application of 12(2), in particular in regard to transborder export of data to non-signatory states.

Chapter IV (Articles 13-17) contains provisions relating to mutual assistance by the national data-protection authorities and assistance to persons who are affected by the use of data in a country other than their country of residence and want to take preventive action. The convention also stipulates that the responsible authorities should not use the data made available for purposes of mutual assistance for purposes other than those for which they are intended.

Chapter V (Articles 18-20) provides for the setting up, after the entry into force of the convention, of a Consultative Committee in which all contracting parties will be represented and which should meet at least every two years. This committee would be responsible in particular for ongoing advice on the implementation of the convention and for proposing necessary amendments.

The final Chapters, VI and VII, (Articles 21-27) contain provisions for possible amendments to the convention and the customary clauses regarding its entry into force and field of application and reservations, termination and registration. The provision on reservations makes it clear that, apart from the exceptions which the individual states may make pursuant to Articles 3(2a), 9(2 and 3) and 12( 3 and 16), no other reservations are possible.

11. In addition to the 'Convention for the protection of individuals with regard to automatic processing of personal data', the Council is expected to devote attention to the need for other provisions in the field of medical data banks, police records and credit records<sup>1</sup>.

12. The European convention will no doubt be criticized, especially because, in Article 3(2a), it allows the signatory states to exclude certain categories of data from its scope. At the same time, it constitutes an important step towards the harmonization of data protection in Europe. Its significance is all the greater since more countries belong to the Council of Europe than to the European Community.

On the other hand, it could well be that some states, in particular those without any data-protection legislation at present, will find even this relatively 'wide-meshed' convention insufficiently flexible.

#### (c) Organization for Economic Cooperation and Development

13. In the summer of 1979, an OECD group of experts presented 'Guidelines on privacy protection and transborder data flows'<sup>2</sup>.

14. The work on the guidelines, which lasted for over two years, ended in their adoption by the OECD Council of Ministers on 23 September 1980<sup>3</sup>. Upon the adoption of the guidelines, by a large majority of the national representatives (18 out of 24 OECD member countries voted for the guidelines, while six abstained but indicated the possibility of acceding at a later date, namely Australia, Canada, Iceland, Ireland, Turkey and the United Kingdom), it was stressed again<sup>4</sup> that the purpose was to safeguard the individual's privacy on the one hand, while ensuring the secure and unimpeded transmission of data, on the other, particular reference being made to transborder data-flow needs in such areas as banking, insurance, aircraft reservations and the despatch of confidential data between the parent company and subsidiaries of multinational undertakings. It was also pointed out that in over half the OECD member countries, data-protection legislation either already existed or had been or soon would be introduced.

<sup>1</sup> cf Doc. 100/79, p. 15, containing further references

<sup>2</sup> OECD Directorate for Science, Technology and Industry, Doc. DSTI"ICCP" 79.40 (DG-14), Paris, 22 June 1979

<sup>3</sup> cf Annex IV, PRESS/A (80) 57

<sup>4</sup> ibid.

## Contents of the guidelines

15. The guidelines are divided into five parts.

Part One contains general considerations. The guidelines apply to both automated and manually stored personal data, in both the public and private sectors (paras. 1(b) and 2). A report on problems connected with transborder flows of non-personal data, on which the group of experts started work at the beginning of 1980, has still to appear.

The scope of the guidelines is restricted to personal data which, because of their nature or the manner in which they are processed, pose a threat to privacy and other individual liberties (para. 2). It also stresses that the guidelines must not be interpreted as preventing the application of different national measures e.g. excluding personal data which obviously do not contain any risk to privacy and individual liberties (3(b)) and restricting application of the guidelines to automatic processing only (3(c)). However, exceptions should be as few as possible (4(a)).

The general statements regarding the scope of the guidelines also include the principle that they are to be regarded as setting an absolute minimum standard and that they may therefore be supplemented by the Member countries by additional, more far-reaching provisions for the protection of privacy and individual liberties (6).

Part Two contains basic principles governing implementation of the guidelines through national legislation. These cover limits on the collection of personal data (7), the relevance of the data to the purpose for which they are to be used; the use made of them, and the need to keep them up to date (8), the need for security safeguards (11) and, lastly, the rights of the data subject vis-à-vis the processors (13).

Part Three lays down the basic principles of free flow, on the one hand, and legitimate restrictions for the purpose of protecting privacy and individual liberties, on the other. It stresses the importance of member countries ensuring that transborder flows of data, including transit through a member country, are free, uninterrupted and secure and avoiding laws or administrative provisions which will create obstacles (16,18). Only when another member country does not apply the guidelines reciprocally or its laws do not provide protection for certain categories of personal data may restrictions be imposed (17).

Part Four sets out rules to be observed by the member countries when adopting provisions in implementation of the guidelines (19) and Part Five concerns the need for international cooperation to ensure that the guidelines are interpreted and implemented in a uniform manner (20-22).



16. The OECD guidelines, like the Council of Europe convention, are designed to establish a balance between the protection of the individual's interests, on the one hand, and economic, international interests in regard to free data flow, on the other. It could be said, however, that they make insufficient provision for the protection of the individual.

There is a wide measure of agreement between the guidelines and the convention, but the latter contains far more detailed rules. As against this, however, the OECD guidelines, which are confined to basic principles, allow the relatively large number of member countries - especially those without data-protection laws - more room for manoeuvre as regards incorporation into domestic law and, unlike the legally binding convention, allows them to assist in the harmonization of data-protection law without time-consuming accession and ratification procedures.

#### (d) Member States of the European Community

A survey of data-protection legislation or work in progress in the Member States of the European Community reveals the following picture:

##### Belgium

17. Since about 1970 efforts have been made to get a new law introduced to provide fuller protection for individuals, notwithstanding a few provisions already existing in the field of civil and public law.

Of the various proposals put forward by the government and other Members of Parliament the Bill<sup>1</sup> tabled in 1976 by Mr Vanderpoorten, which deals in general with threats to private life from technical progress and in Chapters III and IV with the threat from data banks is of particular importance. This Bill is at present under consideration in the Senate's Legal Affairs Committee.

18. The Bill is concerned with the protection of personal data of natural and legal persons in the widest sense, i.e. it also covers data relating indirectly to individuals. It includes the processing of data in data files, i.e. registers of all kinds compiled for the purpose of processing or by means of computers. This, therefore, also includes manual data processing, if it is related in some way to automated processing. Under the terms of the Bill the processing of sensitive data would be subject to a legal ruling or the explicit consent of the data subject and may be carried out by the authorities only within their terms of reference.

---

<sup>1</sup>cf 'Banque de données, Entreprises, Vie Privée', conference proceedings, Namur 1979.

All data banks in Belgium are subject to Belgian law irrespective of the nationality of the keeper. Data banks of supranational organizations are not subject to Belgian jurisdiction. Data banks used by legal persons in compliance with their obligation to publish are excluded, as are those of the National Statistical Office, insofar as they are not used by the government for research purposes.

Registration or a licence from the data protection authority would be required for the operation of data banks in the private sector, and also those in the public sector which are not established to comply with a law. According to this Bill registration alone would be required in the case of those data banks which process data with the consent of the person concerned or - in the public sector - bodies which process data within the framework of their legal responsibilities, on condition in both cases that - save for the examples mentioned - no sensitive data are processed. For all other data banks a licence would have to be obtained, for which the following information would be required:

- the purpose of the data bank,
- the relevance of the data to the purpose for which the data bank is set up,
- the methods of collecting the data,
- the automated processing systems used,
- release of data to third persons,
- the arrangements for ensuring data security,
- the length of time for which the data is to be used.

The data subject would have the right to be informed and to correct and erase his or her data.

A data control authority would monitor compliance with the provisions. It would consist of two bodies (surveillance authority and inspection commission) and would be responsible for registration and licencing. In addition, it would have appropriate rights of access and keep a register of data bank operations.

There is no provision in the Bill for a special body to monitor transborder data flows. Transborder data-flow systems are subject to the same constraints as the national systems.

#### Federal Republic of Germany

19. The 'Law on the protection of personal data from misuse in data-processing' (Federal data protection law) which came into force in 1978 applies to personal data stored and transmitted by all types of data bank in the public and private sectors. Legal persons are not included in the scope of the law.

Monitoring implementation of the law is the responsibility of the Federal Data Ombudsman (Datenschutzbeauftragter), whose Third Activity Report has appeared. Since - apart from provision for inspection to be carried out once the data banks are operating - the law does not provide for a registration or authorization procedure, the Federal Data Ombudsman is brought in only when the misuse of data protection rules has been discovered. In firms employing personal data files for business purposes a member of the staff is specially appointed to see that the rules are not violated.

Before the elections to the German Bundestag of 5 October 1980 bills to amend the Federal data protection law were introduced by the CDU/CSU<sup>2</sup> and SPD<sup>3</sup> groups. These bills will probably not be reintroduced in the new Bundestag. What will probably happen is that the government will introduce a bill to amend the Federal data-protection law taking account of a wide range of demands for the extension of data protection.

In the meantime, all the Länder have issued their own data-protection laws, which embody the basic principles of the Federal Data-Protection Law, even sometimes employing the same words. What distinguishes the data-protection laws of the Länder from the Federal law is that they only cover data-processing by public authorities and bodies in the Land concerned. Only the Federal Data-Protection Law applies to data protection in the non-public sector. Some of the data-protection laws of the Länder - which, except for Rheinland Pfalz (where the Landtag has set up a data protection committee), have their own data-protection ombudsmen - actually go beyond the scope covered by the Federal law; for instance, in regard to compulsory authorization for processing data and the release of data to non-public bodies.

In the Federal data-protection law there are no provisions governing authorization or registration for data-protection purposes for the trans-border transmission of data.

mark

The two laws which were adopted in June 1978 and came into force in January 1979, the Public Authorities' Registers Act and the Private Registers Act, protect automatically processed personal data of natural and legal persons in the public and private sectors.

<sup>1</sup> German Bundestag, 9th electoral term, Doc. 9/93 of 9.1.1981

<sup>2</sup> German Bundestag, 8th electoral term, Doc. 8/3608 of 24.1.1980

<sup>3</sup> German Bundestag, 8th electoral term, Doc. 8/3703 of 27.2.1980

Personal data held in non-automated systems are protected only in the private sector and only if they are such that it can reasonably be claimed that protection from general publication is justified, irrespective of whether they are of a private or financial nature. Moreover, manual data processing is included only if it is carried out

- in the private sector,
- systematically,
- with the type of data referred to above.

Protection does not apply to data stored exclusively for scientific or statistical purposes or for biographical or similar research. In the case of sensitive data this derogation applies exclusively to health data for scientific or statistical purposes.

There is no system of compulsory registration or licensing in the private sector.

Special requirements are imposed, however, in regard to the operations of credit information offices, address agencies and computer service bureaux. Before starting operations such undertakings must apply to be registered with the data protection authority; once this obligation has been discharged the undertaking can begin operations.

The specially set-up data-protection authority, which presents annual reports to parliament on the implementation of the data-protection laws and, in the absence of a general system of compulsory authorization, also investigates misuse, is responsible for authorizing the export of particularly sensitive data.

#### France

21. In France the relevant law on data-processing, files and freedom in the public and private sectors, came into force in 1978. Its provisions on data collection, data security and sensitive data apply both to manually and automatically processed data.

As in the German law, legal persons are not protected.

For both the public and the private sector, the law provides for regular and simplified authorization procedures.

The task of supervising the implementation of the law is carried out by a 'National Commission on Informatics and Freedom', whose 17 members are lawyers and Members of Parliament. The commission also has the right in an emergency to propose to the Conseil d'Etat that all transborder transmissions of personal data be made subject to compulsory authorization.

## Ireland

22. There is no data-protection law at present. Common law and other provisions cover certain aspects of individual privacy.

## Italy

23. Although a parliamentary committee is studying the question of data protection following the presentation of a report of the Privacy Protection Committee, there is no indication that legislation will be adopted in the near future.

## Luxembourg

24. In Luxembourg two important laws have been adopted, the law on personal identity numbers of 30.3.1979 and the law on data protection of 31.3.1979.

Under the former, everyone residing in Luxembourg is allocated a number which is stored in a central register, together with other personal data. The identity number can be used only for internal administrative purposes and to enable the public authorities to contact the person concerned.

The second law protects personal data of natural and legal persons in the public and private sectors if the data are processed electronically.

Since the Luxembourg system is based on a licensing system, authorization must be obtained before private data banks can be established and data banks in the public sector may be established only to comply with a law.

Supervision is in the charge of a Minister, who keeps a national register of all data banks and is assisted by a consultative committee.

The Luxembourg data-protection law contains no specific provision on transborder data transmission.

The Luxembourg law already embodies all the basic principles recommended or laid down in the Council of Europe convention and the OECD guidelines, such as the fair and lawful collection and processing of data, the prohibition on storing sensitive data, with a few exceptions, the obligation on the keeper to inform the data subject and the corresponding obligation on the latter to provide information.

## Netherlands

25. The plan to set up a central population register and the population census of 1970/71 prompted the discussion on data protection in the Netherlands. In 1976 the Koopmans Committee presented its Bill and this has been the subject of further discussion and deliberation in the Dutch Ministry of Justice.

The Bill is to come before parliament in 1981.

26. The Bill concerns protection for personal data of natural persons in the public and private sectors where access to the data can be obtained by automatic means. In addition, it covers systems which permit access to sensitive data and systems which can be used to pass on data to third persons. As regards non-automated processing, the provisions may be applied as they stand or in a modified form.

A data bank may be kept only after it has been registered with the public registry. The registration procedure is divided into three different kinds: simple registration, statutory registration, and licencing. The kind or procedure depends on the identity of the keeper of the data and the kind of data in the particular system.

The simple registration procedure applies to systems which do not contain any sensitive data and which deal with data about memberships, subscribers, customers, suppliers, etc.

The licensing procedure applies to systems which involve the transmission of data to third persons and/or sensitive data in respect of which the data subject's right to be informed and to correct data is to be restricted.

The statutory procedure covers all systems which do not come into either of these two categories.

A public registry will be responsible for supervising implementation of the law.

Under the provisions of the Bill the transmission of data to foreign data systems and the procurement of data from such systems is, with few exceptions, prohibited.

#### United Kingdom

27. The discussion in the United Kingdom centres round the Lindop report drawn up by the Committee on Data Protection set up under the auspices of the Home Office<sup>1</sup>.

This report is not in the form of a Bill but presents a number of recommendations which are intended to serve as the basis of future data-protection law.

---

<sup>1</sup> Home Office, Report of the Committee on Data Protection, Chairman: Sir Norman Lindop, London, December 1978, Cmnd 7341

---

28. The rules proposed concern the protection of data of natural persons in the public and private sectors where automated data processing is involved.

The recommendations do not provide for registration or authorization, although it seems likely that such provision would be included in the data-protection laws.

Supervision of implementation would be the responsibility of a Data Protection Authority, which - to preserve a flexible approach towards the various types and uses of data processing - could lay down rules applicable to individual users, groups of users, and individual systems or groups of systems.

A notable feature of the report is that it stresses transborder transmission of data as a fundamental reason for introducing national rules. It is envisaged that the Data Protection Authority would be invested with the right, within its terms of reference, to issue rules on the transmission of data abroad.

#### Greece

29. There have been no developments since the Bayerl report was drawn up; it is unlikely that data-protection legislation will be introduced in the foreseeable future.

#### (e) Other member countries of the Council of Europe

The position in regard to data protection in the other member countries of the Council of Europe is as follows:

### Norway

30. The Norwegian law, which covers manual and automated personal data files in the public and private sectors in respect of both natural and legal persons, has been in force since its adoption in May 1978. Licences are required for transborder data transmission and also for the manual and automated storage of sensitive personal data. The Data Surveillance Service monitors compliance with the law's provisions.

### Austria

31. The Federal Data Protection Law of 1978 applies to the automated processing of personal data of legal and natural persons in the public and private sectors.

The operation of data banks is subject to prior registration or - for certain kinds of data - a simplified system of notification.

The Federal Data Protection Commission monitors observance of the rules.

The October 1979 version of the law includes a section on transborder data flow. This makes it obligatory to obtain the Data Protection Commission's authorization before exporting data, such authorization being granted on the basis of specified criteria. This also applies when information is procured from abroad by a processing agency stationed in Austria or simply when one operation in the processing is carried out abroad.

### Portugal and Spain

32. In Portugal and Spain certain aspects of privacy and personal freedom are protected by constitutional provisions; in Portugal a Bill on data protection is also being drawn up.

### Sweden

33. The data-protection law which was adopted in 1973 and came into force



in 1974 and which protects personal data of natural persons in the public and private sectors, when the data are collected by means of automated processing in registers, lists or otherwise, has been subsequently reviewed by a committee specially set up for the purpose.

The amendments proposed by the committee have been adopted and came into force on 1 July 1979.

One of the changes takes into account the fact that the majority of automated data banks do not injure the interests of the data subjects. Consequently, the operation of such banks is no longer subject to authorization by the Data Inspection Board, but only to a simplified registration procedure. Specific criteria are laid down for granting authorization in the case of other kinds of data bank, account being taken of the nature of the data and the number of persons concerned. Authorization is also subject to strict criteria in regard to the purpose for which data are stored. In particular, in the case of storage and transmission of data concerning persons who have no business or employment connection with the keeper, consent is now given only where there is special justification.

Furthermore, from 1 July 1981 only State agencies will be permitted to establish address lists of the population and release details of them. The same will apply too to particularly sensitive data.

The rights of the data subject have also been greatly strengthened. Thus, the data subject now has a right to be told that no data concerning him are being stored. As a further protection of the individual, there is a provision requiring the keeper of the data bank to supplement entries or add relevant additional information.

The Data Inspection Board, whose responsibility for issuing licences extends to transborder data flows, is also empowered to forbid the operation of data banks where the interests of privacy or personal freedom are injured or threatened.

The amendments to the data-protection law did not take account of the committee's proposal to exempt from its provisions files set up for research or statistical purposes.

#### Switzerland

34. One result of the federal structure of Switzerland is that data-protection laws exist only at cantonal level. A government report is being drawn up in the public sector committee for administrative and Federal institutions with a view to the adoption of a general Federal law.

Remaining member countries of the Council of Europe

35. The rapporteur has no information regarding developments on data protection in Cyprus, Iceland, Liechtenstein, Malta or Turkey.

(f) OECD member countries

The position in regard to data protection in some OECD countries is as follows:

Australia

36. In Australia data-protection legislation exists only at the level of the Federal states. A government report on the subject is being drawn up.

Finland

37. Now that the importance of data protection is recognized, a government report is being drawn up on the subject.

Yugoslavia

38. In Yugoslavia, too, an associate member country of the OECD, a government report is being drawn up.

Canada

39. In Canada, data-protection laws have recently come into force both at Federal State level and in the individual states.

The storing abroad of personal data relating to Canadian nationals is prohibited, as is the transmission abroad of personal data.

USA

40. Responsibility for legislation in the United States is divided among many different bodies. This means, for instance, that there are no definitive Federal rules governing data processing in industry. The Federal Fair Credit Reporting Act lays down only minimal requirements applicable throughout the Federation and allows the states to introduce additional provisions if these are compatible with it. The response of the states has varied.

The laws governing the data practice of banks and other financial institutions also differ from state to state.

Only a few states have introduced data-protection legislation relating to insurance and employment relationships.

For their own administrations some states have adopted Privacy Acts or Fair Information Practices Acts, which cover the collection, storage, use and release of personal data. A few other states have introduced rules for protection of data in specific technical fields.

The National Conference of Commissioners on Uniform State Laws has almost finished drafting a model data-protection law for the individual states.

At Federal level there is the Privacy Act of 1974, which applies to most administrative bodies of the Federation. In addition, a number of Federal laws protect the confidentiality of certain files e.g. the tax authorities, statistical offices and the narcotics control authorities. Stringent data-protection measures have been introduced for schools and colleges. Data protection in the credit sector is provided by the aforementioned Fair Credit Reporting Act and other laws (Equal Credit Opportunity Act, Fair Credit Billing Act, Fair Debt Collection Practices Act and - in relation to the administration - the Right to Financial Privacy Act).

The approach to legislation is much more sectoral in character than that of most European laws; the rules are therefore generally narrower in scope as regards subject and legal implications and there are few laws of a comprehensive nature. This has the advantage of greater concreteness and practical relevance.

A number of notable proposals have been submitted to Congress recently, on the initiative partly of the President and partly of individual Representatives and Senators who have taken up the subject.

At present three competing Bills on the protection of medical data are pending.

Possible solutions to problems presented by a totally new technology, which has scarcely even got off the ground yet, are contained in the draft for a Fair Financial Information Practices Act; this is designed to protect data which becomes available in the course of payment transactions, as will be possible in future with home terminals.

Also of interest is the call for an FBI 'Charter', on which Senator Edward Kennedy has submitted a proposal.

The debate on data protection in the USA is influenced by the mounting criticism of bureaucratic practices, which is directed not only at lack of coordination and duplication between many government departments, but also at any move to extend State activity. This hostility has also prevented the establishment to date of a central data-protection supervisory board

proposed by, among others, the Privacy Protection Study Commission. Such boards exist only in certain states. The lack of a central supervisory authority has also meant that the USA has not as yet participated in the task of establishing international cooperation between data-protection authorities undertaken elsewhere.

### III. Questions to be decided

41. Following this review of the present position with regard to data-protection, we need to examine some questions of substantive law.

Since the Council of Europe's draft convention for the protection of individuals with regard to automated data-files constitutes a body of provisions which meets with the approval of the majority of the Member States' governments, including those of the European Community, the question arises whether or not the demands contained in the European Parliament's resolution of 8 May 1979 have already been met in this convention and whether - in the event of a Community directive being drawn up - these demands are compatible with the provisions of the convention.

#### (a) Compatibility of the provisions of the Council of Europe's convention with the European Parliament's demands

42. The demands contained in the European Parliament's resolution of May 1979 are aimed at the adoption of Community legislation to provide its citizens with maximum protection. They include the recommendation that automated or manual personal data banks should be subject to prior registration or authorization<sup>1</sup>.

The latter demand could lead to conflict with the Council of Europe convention.

This convention refrains from such a radical measure; instead, it stresses in the preamble itself the equally important principles of safeguarding the individual's interests and ensuring free movement of information. Consequently, there is nowhere in the text of the convention any provision making the operation of personal data banks subject to prior registration or authorization. Article 11 of the convention emphasizes, however, that this chapter of the convention is not to be interpreted as 'restricting or otherwise prejudicing the possibility open to a Contracting Party to grant those concerned a greater measure of protection than that provided in this Convention'. If it is presumed that the introduction of mandatory prior registration or authorization goes further than the convention, and that it is to be regarded as a protective measure safeguarding the interests of both the individual concerned and the State, and bearing in mind that the convention allows for optional extension of data-protection measures by a discretionary clause, it would seem possible to meet the European Parliament's

<sup>1</sup> cf. Doc. 100/79, A. Recommendation I(1)

demands by means of Community provisions without coming into conflict with the Council of Europe convention.

43. Although Article 11 of the convention expressly leaves the signatories free to grant 'those concerned a greater measure of protection than that provided' in the convention, this applies only to its Chapter I. This chapter deals with the scope of the convention, the persons protected, the collection, storage, processing and erasure of data, sensitive data, data protection and the rights of those concerned. There is extensive agreement here between the European Parliament's demands of May 1979 and the convention's provisions. Thus, the starting-point in both cases is the need to protect natural persons. The convention also, however, in Article 3(2b), allows corresponding rights to be granted to legal persons. In line, too, with the European Parliament's ideas of the Community legislation required, protection under the convention will cover both the private and the public sectors, since the individual is entitled to protection in either sector. There is also substantial agreement with regard to the commitments entered into by the signatories concerning the use of data and the rights of data subjects. In its Article 3(2c), the convention, which applies mandatorily only to the field of automated data processing, specifically allows manual processing to be included in the scope of national legislation. In this, again, it is in conformity with the European Parliament's First Report of May 1979.

The possibility provided in Article 3 (2a) for the signatories to exclude certain categories of data from the scope of the convention is compatible with the European Parliament's demands, since in principle the convention can be deemed applicable to all kinds of automated personal data.

The fact that Chapter I of the convention allows for the adoption of more favourable rules makes it possible for the Community, in regard to the above-mentioned points, to satisfy the demand for Community law to provide the highest possible level of data protection.

44. On the other hand, the European Parliament's demands could conflict with the provisions of the convention in regard to prior authorization for trans-border data transmission.

Parliament recommended that the transborder transmission of data within the Community should not be subject to special arrangements and should only need to be reported to the Community's control body, whereas the export of data from the Community's territory would require the authorization of the Community's data protection authority.

The Council of Europe convention, too, according to Article 12(2), does not consider it possible to restrict the transmission of data between the signatories solely for the purpose of protecting the interests of the

individual. If the European Parliament's demands were met, the Member States of the Community would be obliged - since, being member countries of the Council of Europe, they will be signatories to the European convention - to observe both the provisions of the convention and those of the Community. Since the Council of Europe is numerically the larger of the two communities of states, this would mean that, under Community provisions, the export of data to member countries of the Council of Europe outside the Community would be subject to the authorization of the Community's data-protection authority, while, under the convention's provisions, the Member States of the Community would be obliged at the same time to permit the free transmission of data across borders within the larger organization of 21 States.

Under Article 12(3b) the signatories to the European convention can impose limits on the transborder export of data to non-signatory States.

45. To achieve compatibility between Parliament's wishes and the provisions of the convention it would therefore seem advisable to adopt Community provisions protecting personal data and permitting the transborder transmission of data without authorization between the Member States of the Community on the one hand and the other member countries of the Council of Europe on the other inasfar as the latter had signed the Council of Europe Convention on data protection.

However, the demand that transborder data transmission within this European zone should be subject to notification simply for the purpose of registration seems compatible with Article 12(2) of the convention.

46. It may be seen from Article 12(3b) that the convention does not conflict with the European Parliament's demand that prior authorization be made obligatory for the export of data to third countries, insofar as these countries are not members of the Council of Europe.

#### (b) Need for Community law

47. The introduction of Community legislation in the field of data protection is called for 'to the extent required for the proper functioning of the common market' (Art.3(h) of the EEC Treaty). It is the Community's responsibility to eliminate disturbances which can arise in the operation of a Community which is in the process of becoming a single uniform economic zone because economic activity is governed by different national legal systems valid only within the national territories. The foregoing survey has shown that data protection norms vary considerably from one Member State to another and that the common market in the data-processing and transmission field, and also the freedom to provide services in this field, can be severely restricted and impeded. This is confirmed by the findings of the Council of Europe and the OECD.

The differences between Member States in regard to the nature and stringency of their legislative provisions and their actual supervision and control arrangements can be prejudicial both to the persons whose data are stored or processed and to the data banks. Transborder competition in data banks and free data flow within the Community are possible only if data protection is harmonized. The fact that the storing and processing of data are services like any others justifies the assertion that the proper functioning of the common market can be jeopardized if data-protection law is not placed on a uniform substantive basis in conformity with Community law.

However, it is unrealistic to suppose there can be freedom of data transmission without adequate data protection. That would be contrary not only to national constitutions and laws, but also to the objective laid down in the preamble to the EEC Treaty concerning the constant improvement of the living conditions of our peoples and to the Joint Declaration by the President of the Council, Parliament and Commission 'on the protection of human rights and fundamental freedoms'.

The harmonization of national provisions in the field of data protection is therefore necessary for the proper functioning of the common market in the field of data storage, processing and transmission.

The legal basis for such harmonization is first and foremost Article 100 of the EEC Treaty. It is therefore necessary to consider whether the legal provisions which are to be harmonized directly affect the establishment or functioning of the common market. In order to demonstrate that they do directly affect it, it is not necessary, in the frequently expressed view of the European Court of Justice (e.g. Case 19/77 Miller v. Commission, [1978] ECR 131), to show that a particular course of conduct has prejudiced trade between the Member States, but only that the conduct or agreement in question is capable of having such an effect. It is a matter of foreseeability. The decisive factor is the probability 'based on a number of objective legal or actual factors', of direct or indirect, present or potential influence. In this sense, the protection of the individual and the harmonization of the different national data-protection provisions to that end do directly affect the conduct of the storer, processor, transmitter and recipient of data.

48. Since, with the Council of Europe convention and the OECD guidelines, concrete steps have been taken meanwhile towards the adoption and harmonization of data-protection law, it is necessary to ask whether Community provisions are still needed.

This question must be answered in the affirmative, because

- the OECD decisions have no binding force, although they may

eventually be brought into force in most countries with a highly developed data-processing industry;

- accession to the international convention of the Council of Europe by the 21 member countries is optional; furthermore, ratification is likely, on past evidence, to be a lengthy process;
- the Council of Europe convention represents, admittedly, the most far-reaching arrangement at international level for instituting or harmonizing data-protection law in the signatory states, but it falls short of the European Parliament's ideas to date on the Community provisions required;
- many of the provisions of the European Convention for strengthening data protection are only optional and permit restrictions by individual states;
- Community rules are needed to regulate transborder data-flow between the Member States of the Community and its institutions and organs, on the one hand, and the rest of the signatories to the European convention, on the other;
- Community provisions will ensure a higher level of harmonization.

(c) Accession of the European Community to the Council of Europe's Convention

49. There is, finally, the question of whether, after the introduction of Community provisions in the data-protection field, the accession of the European Community to the convention itself still appears feasible or, for that matter, desirable.

A precondition for its possible accession is that the Community's jurisdiction should extend to the field in question. This can be confirmed by reference both to the principles contained in the preamble to the EEC Treaty and to Article 3(h) of the Treaty, which speaks of the harmonization of national laws for the purpose of ensuring the proper functioning of the common market. There is no doubt that the use of modern technologies in the data-processing field has an influence on all sectors of the common market.

Furthermore, the Community as such must have the legal authority to accede to the European convention. The legal basis which permits the European Community's participation in international trade is its status as a subject of international law. The central provision of Article 228 of the EEC Treaty, which states that the Community may itself conclude agreements where provided for in the EEC Treaty, has been considerably widened by



invoking Article 235 of the Treaty, the 'implied powers' theory and the important decision of the European Court of Justice of 31 March 1971<sup>1</sup> in which the Court ruled that the Community has a general treaty-making power.

Another precondition would be that, at the time of the Community's accession to the Council of Europe convention, all the Member States would have to be signatories to that convention. Given the wide measure of agreement existing already, this precondition already seems capable of being met.

50. The question of the legal competence of the Community as such to accede to the convention having been answered in the affirmative, the question now arises as to the need for such a step, if Community provisions already exist.

The European convention constitutes a body of provisions which, by comparison with the Community provisions advocated, fall short of the European Parliament's idea of maximum protection. One may, therefore, question whether there is any point in subscribing to a 'lesser' body of norms where a 'greater' one already exists. This question, which need not be definitively answered yet, could be relevant with regard to data protection in the Community field as such, that is, its institutions and organs. If, that is, the Member States of the European Community and the member countries of the Council of Europe have already introduced data-protection laws, a similar right should also exist for the Community as a legal person, particularly if the directive to be adopted is addressed exclusively to the Member States and does not cover the Community's institutions and organs.

51. Although, in the event of more far-reaching rules being introduced for the Member States, it is unlikely that the Community's institutions and organs would adopt a negative attitude to the protection of their own data, the Community's accession to the convention or the introduction of a regulation directed at the institutions and organs might be desirable to ensure full data protection.

#### IV. Conclusions

52. The above observations and review of existing norms in the field of data protection make it clear that more far-reaching norms are needed in the

---

<sup>1</sup> Case 22/70 (ERTA) [1971] ECR 263

Community field than those contained in the Council of Europe convention and the OECD guidelines.

Proceeding from the conviction that modern technologies constitute a serious threat to the rights of the individual, in particular the right to privacy, and in the interests of achieving a high degree of harmonization of Member States' data-protection laws, this committee believes that a Community directive is as urgently needed as ever before to provide the highest possible level of protection.

53. When issuing such a directive, care must be taken to ensure that
- the protection from modern data-processing techniques applies equally to the private and the public sectors;
  - this protection is extended to all transmissions of personal data across frontiers;
  - notification of the person concerned is made obligatory;
  - the directive introduces liability for damage caused and
  - it makes the operation of data banks subject to prior notification and authorization.
54. A Community body must be set up to regulate the detailed procedures for transmission of data and having sole responsibility for monitoring the application of the Community norms.
55. As an initial contribution to the creation and/or harmonization of European data-protection laws on the basis of the draft convention for the protection of individuals with regard to automated data-files, it would be desirable to call on the Member States' governments and parliaments to ratify that convention as soon as possible.
56. As mentioned already, it is not possible at this stage for a decision to be made on the accession of the European Community in its own right to the Council of Europe convention. It might, however, be worth considering its accession or the adoption of a regulation on data protection for the Community field, for the purpose of ensuring a comprehensive body of data-protection laws which would also cover the lawful processing of the Community's own data by its institutions and organs.

MOTION FOR A RESOLUTION (Doc. 1-116/80)

tabled by Mr Glinne, Mr Brandt, Mr Colla, Mr Vernimmen, Mrs Lizin, Mrs Roudy, Mrs Charzat, Mr Josselin, Mr Sarre, Mr Moreau, Mrs Weber, Mrs Focke, Mrs Castle, Mrs Gredal, Mrs Van den Heuvel, Mrs Viehoff, Mr Dido, Mr Schmid, Mr Lezzi, Mr Hänsch, Mr Schwartzenberg, Mr Delors, Mr Walter, Mr Linde, Mrs Krouwel-Vlam, Mrs Hoff, Mr Collins, Mr Key, Mr Griffiths, Mr Muntingh, Mr Albers and Mr von der Vring

on behalf of the Socialist Group  
pursuant to Rule 25 of the Rules of Procedure

on the protection of individuals against data processing

The European Parliament,

- anxious to protect the rights of the individual and to safeguard fundamental freedoms,
- concerned at the legal problems raised by technical developments, particularly in the field of data processing,
- considering that the present situation calls for urgent and effective remedies,

Requests the Member States of the European Economic Community which have ratified the Convention on Human Rights and Fundamental Freedoms to adopt a protocol N° 6 to the Convention introducing standard implementing rules for Article 8 of the Convention, protecting the private life of individuals against the use and dangers of data processing and data banks, as drafted and proposed by the International Union of Lawyers on 14 September 1979.

MOTION FOR A RESOLUTION (Doc. 1-103/80), tabled by Mrs Roudy, Mr Schwartz, Mr Colla and Mr Glinne, pursuant to Rule 25. of the Rules of Procedure on the protection of private life - control of telephone tapping -

The European Parliament.

- whereas, pursuant to Article 12 of the Universal Declaration of Human Rights (stipulating that there shall be no arbitrary interference in the private life of citizens) each individual is entitled to judicial protection against any such interference or activities,
  - having regard to the European Convention of Human Rights (in particular the principle of respect for private life ),  
having regard to the OECD resolution of 22 July 1979,  
noting that modern technology presents a serious threat to individual rights and in particular to the right to respect for private life,
  - noting that new techniques, the use of miniaturized devices and the proliferation of spying techniques facilitate interference in the private life of individuals,  
noting that in certain Community countries, national legislation protects citizens against the abusive use of data-processing techniques,
  - having regard to Article 100 of the EEC Treaty on the harmonization of national legislative provisions,
  - believing that where such national legislative provisions exist, they must be not only harmonized but also improved,
  - considering that although the EEC is an economic and trading Community, it must be in a position to avoid undesirable secondary effects by protecting European citizens through uniform and effective general provisions on data-processing,
  - considering that the transmission of data must, as a matter of general principle, be governed by a legal basis and not by considerations of a technical nature,
1. Hopes that a debate will be held in the European Parliament on the abuse of data-processing;
  2. Is of the opinion that it is urgently necessary to adopt a Community directive which will not only harmonize at the highest level existing statutory provisions but will further improve them by ensuring that protection against such techniques is identical in the private and public sectors, extends to all personal information beyond national frontiers, stipulates an obligation to inform the person concerned and, where appropriate, provides for responsibility for damage suffered to be established;
  3. Considers it essential to create a Community juridical agency responsible for monitoring the application of the provisions contained in the directive and for regulating the procedures for the transmission of data.

CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC  
PROCESSING OF PERSONAL DATA

PREAMBLE

The member States of the Council of Europe, signatory hereto,

Considering that the aim of the Council of Europe is to achieve greater unity between its members, based in particular on respect for the rule of law, as well as human rights and fundamental freedoms ;

Considering that it is desirable to extend the safeguards for everyone's rights and fundamental freedoms, and in particular the right to the respect for privacy, taking account of the increasing flow across frontiers of personal data undergoing automatic processing ;

Reaffirming at the same time their commitment to freedom of information regardless of frontiers ;

Recognising that it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples,

Have agreed as follows :

CHAPTER I — GENERAL PROVISIONS

Article 1

*Object and purpose*

The purpose of this convention is to secure in the territory of each Party for every individual, whatever his nationality or residence, respect for his rights and fundamental freedoms, and in particular his right to privacy, with regard to automatic processing of personal data relating to him ("data protection").

Article 2

*Definitions*

For the purposes of this convention :

a. "personal data" means any information relating to an identified or identifiable individual ("data subject") ;

b. "automated data file" means any set of data undergoing automatic processing ;

c. "automatic processing" includes the following operations if carried out in whole or in part by automated means : storage of data, carrying out of logical and/or arithmetical operations on those data, their alteration, erasure, retrieval or dissemination ;

d. "controller of the file" means the natural or legal person, public authority, agency or any other body who is competent according to the national law to decide what should be the purpose of the automated data file, which categories of personal data should be stored and which operations should be applied to them.

### Article 3

#### *Scope*

1. The Parties undertake to apply this convention to automated personal data files and automatic processing of personal data in the public and private sectors.

2. Any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, or at any later time, give notice by a declaration addressed to the Secretary General of the Council of Europe :

a. that it will not apply this convention to certain categories of automated personal data files, a list of which will be deposited. In this list it shall not include, however, categories of automated data files subject under its domestic law to data protection provisions. Consequently, it shall amend this list by a new declaration whenever additional categories of automated personal data files are subjected to data protection provisions under its domestic law ;

b. that it will also apply this convention to information relating to groups of persons, associations, foundations, companies, corporations and any other bodies consisting directly or indirectly of individuals, whether or not such bodies possess legal personality ;

c. that it will also apply this convention to personal data files which are not processed automatically.

3. Any State which has extended the scope of this convention by any of the declarations provided for in sub-paragraph 2.b or c above may give notice in the said declaration that such extensions shall apply only to certain categories of personal data files, a list of which will be deposited.

4. Any Party which has excluded certain categories of automated personal data files by a declaration provided for in sub-paragraph 2.a above may not claim the application of this convention to such categories by a Party which has not excluded them.

5. Likewise, a Party which has not made one or other of the extensions provided for in sub-paragraphs 2.b and c above may not claim the application of this convention on these points with respect to a Party which has made such extensions.

6. The declarations provided for in paragraph 2 above shall take effect from the moment of the entry into force of the convention with regard to the State which has made them if they have been made at the time of signature or deposit of its instrument of ratification, acceptance, approval or accession, or three months after their receipt by the Secretary General of the Council of Europe if they have been made at any later time. These declarations may be withdrawn, in whole or in part, by a notification addressed to the Secretary General of the Council of Europe. Such withdrawals shall take effect three months after the date of receipt of such notification.

## CHAPTER II — BASIC PRINCIPLES FOR DATA PROTECTION

### Article 4

#### *Duties of the Parties*

1. Each Party shall take the necessary measures in its domestic law to give effect to the basic principles for data protection set out in this chapter.

2. These measures shall be taken at the latest at the time of entry into force of this convention in respect of that Party.

**Article 5**  
*Quality of data*

Personal data undergoing automatic processing shall be :

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

**Article 6**  
*Special categories of data*

Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.

**Article 7**  
*Data security*

Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination.

**Article 8**  
*Additional safeguards for the data subject*

Any person shall be enabled :

- a. to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file ;
- b. to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form ;
- c. to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention ;
- d. to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.

**Article 9**  
*Exceptions and restrictions*

1. No exception to the provisions of Articles 5, 6 and 8 of this convention shall be allowed except within the limits defined in this article.

2. Derogation from the provisions of Articles 5, 6 and 8 of this convention shall be allowed when such derogation is provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of :

a. protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences ;

b. protecting the data subject or the rights and freedoms of others.

3. Restrictions on the exercise of the rights specified in Article 8, paragraphs b, c and d, may be provided by law with respect to automated personal data files used for statistics or for scientific research purposes when there is obviously no risk of an infringement of the privacy of the data subjects.

#### Article 10

##### *Sanctions and remedies*

Each Party undertakes to establish appropriate sanctions and remedies for violations of provisions of domestic law giving effect to the basic principles for data protection set out in this chapter.

#### Article 11

##### *Extended protection*

None of the provisions of this chapter shall be interpreted as limiting or otherwise affecting the possibility for a Party to grant data subjects a wider measure of protection than that stipulated in this convention.

### CHAPTER III — TRANSBORDER DATA FLOWS

#### Article 12

##### *Transborder flows of personal data and domestic law*

1. The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.

2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.

3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2 :

a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection ;

b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.



## CHAPTER IV — MUTUAL ASSISTANCE

### Article 13

#### *Co-operation between Parties*

1. The Parties agree to render each other mutual assistance in order to implement this convention.
2. For that purpose :
  - a. each Party shall designate one or more authorities, the name and address of each of which it shall communicate to the Secretary General of the Council of Europe ;
  - b. each Party which has designated more than one authority shall specify in its communication referred to in the previous sub-paragraph the competence of each authority.
3. An authority designated by a Party shall at the request of an authority designated by another Party :
  - a. furnish information on its law and administrative practice in the field of data protection ;
  - b. take, in conformity with its domestic law and for the sole purpose of protection of privacy, all appropriate measures for furnishing factual information relating to specific automatic processing carried out in its territory, with the exception however of the personal data being processed.

### Article 14

#### *Assistance to data subjects resident abroad*

1. Each Party shall assist any person resident abroad to exercise the rights conferred by its domestic law giving effect to the principles set out in Article 8 of this convention.
2. When such a person resides in the territory of another Party he shall be given the option of submitting his request through the intermediary of the authority designated by that Party.
3. The request for assistance shall contain all the necessary particulars, relating *inter alia* to :
  - a. the name, address and any other relevant particulars identifying the person making the request ;
  - b. the automated personal data file to which the request pertains, or its controller ;
  - c. the purpose of the request.

### Article 15

#### *Safeguards concerning assistance rendered by designated authorities*

1. An authority designated by a Party which has received information from an authority designated by another Party either accompanying a request for assistance or in reply to its own request for assistance shall not use that information for purposes other than those specified in the request for assistance.
2. Each Party shall see to it that the persons belonging to or acting on behalf of the designated authority shall be bound by appropriate obligations of secrecy or confidentiality with regard to that information.

3. In no case may a designated authority be allowed to make under Article 14, paragraph 2, a request for assistance on behalf of a data subject resident abroad, of its own accord and without the express consent of the person concerned.

#### Article 16

##### *Refusal of requests for assistance*

A designated authority to which a request for assistance is addressed under Articles 13 or 14 of this convention may not refuse to comply with it unless :

- a. the request is not compatible with the powers in the field of data protection of the authorities responsible for replying ;
- b. the request does not comply with the provisions of this convention ;
- c. compliance with the request would be incompatible with the sovereignty, security or public policy (*ordre public*) of the Party by which it was designated, or with the rights and fundamental freedoms of persons under the jurisdiction of that Party.

#### Article 17

##### *Costs and procedures of assistance*

1. Mutual assistance which the Parties render each other under Article 13 and assistance they render to data subjects abroad under Article 14 shall not give rise to the payment of any costs or fees other than those incurred for experts and interpreters. The latter costs or fees shall be borne by the Party which has designated the authority making the request for assistance.
2. The data subject may not be charged costs or fees in connection with the steps taken on his behalf in the territory of another Party other than those lawfully payable by residents of that Party.
3. Other details concerning the assistance relating in particular to the forms and procedures and the languages to be used, shall be established directly between the Parties concerned.

### CHAPTER V — CONSULTATIVE COMMITTEE

#### Article 18

##### *Composition of the committee*

1. A Consultative Committee shall be set up after the entry into force of this convention.
2. Each Party shall appoint a representative to the committee and a deputy representative. Any member State of the Council of Europe which is not a Party to the convention shall have the right to be represented on the committee by an observer.
3. The Consultative Committee may, by unanimous decision, invite any non-member State of the Council of Europe which is not a Party to the convention to be represented by an observer at a given meeting.

#### Article 19

##### *Functions of the committee*

The Consultative Committee :

- a. may make proposals with a view to facilitating or improving the application of the convention ;

- b. may make proposals for amendment of this convention in accordance with Article 21 ;
- c. shall formulate its opinion on any proposal for amendment of this convention which is referred to it in accordance with Article 21, paragraph 3 ;
- d. may, at the request of a Party, express an opinion on any question concerning the application of this convention.

#### Article 20

##### *Procedure*

1. The Consultative Committee shall be convened by the Secretary General of the Council of Europe. Its first meeting shall be held within twelve months of the entry into force of this convention. It shall subsequently meet at least once every two years and in any case when one-third of the representatives of the Parties request its convocation.
2. A majority of representatives of the Parties shall constitute a quorum for a meeting of the Consultative Committee.
3. After each of its meetings, the Consultative Committee shall submit to the Committee of Ministers of the Council of Europe a report on its work and on the functioning of the convention.
4. Subject to the provisions of this convention, the Consultative Committee shall draw up its own Rules of Procedure.

### CHAPTER VI — AMENDMENTS

#### Article 21

##### *Amendments*

1. Amendments to this convention may be proposed by a Party, the Committee of Ministers of the Council of Europe or the Consultative Committee.
2. Any proposal for amendment shall be communicated by the Secretary General of the Council of Europe to the member States of the Council of Europe and to every non-member State which has acceded to or has been invited to accede to this convention in accordance with the provisions of Article 23.
3. Moreover, any amendment proposed by a Party or the Committee of Ministers shall be communicated to the Consultative Committee, which shall submit to the Committee of Ministers its opinion on that proposed amendment.
4. The Committee of Ministers shall consider the proposed amendment and any opinion submitted by the Consultative Committee and may approve the amendment.
5. The text of any amendment approved by the Committee of Ministers in accordance with paragraph 4 of this article shall be forwarded to the Parties for acceptance.
6. Any amendment approved in accordance with paragraph 4 of this article shall come into force on the thirtieth day after all Parties have informed the Secretary General of their acceptance thereof.

## CHAPTER VII — FINAL CLAUSES

### Article 22

#### *Entry into force*

1. This convention shall be open for signature by the member States of the Council of Europe. It is subject to ratification, acceptance or approval. Instruments of ratification, acceptance or approval shall be deposited with the Secretary General of the Council of Europe.

2. This convention shall enter into force on the first day of the month following the expiration of a period of three months after the date on which five member States of the Council of Europe have expressed their consent to be bound by the convention in accordance with the provisions of the preceding paragraph.

3. In respect of any member State which subsequently expresses its consent to be bound by it, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of the deposit of the instrument of ratification, acceptance or approval.

### Article 23

#### *Accession by non-member States*

1. After the entry into force of this convention, the Committee of Ministers of the Council of Europe may invite any State not a member of the Council of Europe to accede to this convention by a decision taken by the majority provided for in Article 20.d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the committee.

2. In respect of any acceding State, the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

### Article 24

#### *Territorial clause*

1. Any State may at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, specify the territory or territories to which this convention shall apply.

2. Any State may at any later date, by a declaration addressed to the Secretary General of the Council of Europe, extend the application of this convention to any other territory specified in the declaration. In respect of such territory the convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of receipt of such declaration by the Secretary General.

3. Any declaration made under the two preceding paragraphs may, in respect of any territory specified in such declaration, be withdrawn by a notification addressed to the Secretary General. The withdrawal shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of such notification by the Secretary General.

### Article 25

#### *Reservations*

No reservation may be made in respect of the provisions of this convention.

## Article 26

### *Denunciation*

1. Any Party may at any time denounce this convention by means of a notification addressed to the Secretary General of the Council of Europe.
2. Such denunciation shall become effective on the first day of the month following the expiration of a period of six months after the date of receipt of the notification by the Secretary General.

## Article 27

### *Notifications*

The Secretary General of the Council of Europe shall notify the member States of the Council and any State which has acceded to this convention of :

- a. any signature ;
- b. the deposit of any instrument of ratification, acceptance, approval or accession ;
- c. any date of entry into force of this convention in accordance with Articles 22, 23 and 24 ;
- d. any other act, notification or communication relating to this convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Strasbourg, the 28th day of January 1981, in English and in French, both texts being equally authoritative, in a single copy which shall remain deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe and to any State invited to accede to this Convention.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Strasbourg, le 28 janvier 1981, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe et à tout Etat invité à adhérer à la présente Convention.

OECD PRESS RELEASE

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

PRESS/A(80)57

Paris, 2nd October 1980

OECD GUIDELINES ON PRIVACY PROTECTION  
AND TRANSBORDER DATA FLOWS

Every person should have the right to know what data relating to him or her are stored and where they are stored, and to have access to them, and if appropriate to have them corrected or erased;

all personal data should be secured against unauthorised access or disclosure or other forms of abuse;

personal data transmitted to other OECD countries should receive similar protection as in the home country, and such transborder data flows should be "uninterrupted and secure".

These basic principles are among a set of "Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data" just adopted by the Council of the OECD. They are contained in a Council Recommendation to Governments aimed at harmonising privacy protection laws in OECD Member countries.

The Guidelines were developed over a period of 2 years by a Group of Experts, under the chairmanship of The Hon. Justice M.D. Kirby, Chairman of the Australian Law Reform Commission.

Privacy Protection laws have been introduced, or will be introduced shortly, in just over half of OECD countries (1). There is a danger that legal disparities could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in such areas as banking, insurance, aircraft reservations and the despatch of confidential data between the parent company and subsidiaries of multinational enterprises.

The OECD Guidelines, the text of which is attached to this release, apply to both automated and manually stored personal data, both in the public and private sectors. Eighteen of the twenty-four OECD Member governments have adopted the Council Recommendation. From the six which abstained (Australia, Canada, Iceland, Ireland, Turkey, the United Kingdom), most of them have indicated that they were contemplating the possibility of adhering to the Recommendation soon.

- 
- (1) Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills.

RECOMMENDATION OF THE COUNCIL OF THE OECD (\*)  
CONCERNING GUIDELINES GOVERNING THE PROTECTION OF  
PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

The Council,

Having regard to articles 1(c), 3(a) and 5(b) of the Convention on the Organisation for Economic Co-operation and Development of 14th December, 1960;

Recognising:

that, although national laws and policies may differ, Member countries have a common interest in protecting privacy and individual liberties, and in reconciling fundamental but competing values such as privacy and the free flow of information;

that automatic processing and transborder flows of personal data create new forms of relationships among countries and require the development of compatible rules and practices;

that transborder flows of personal data contribute to economic and social development;

that domestic legislation concerning privacy protection and transborder flows of personal data may hinder such transborder flows;

Determined to advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries;

RECOMMENDS

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;
2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.

---

(\*) The Australian, Canadian, Icelandic, Irish, Turkish and United Kingdom Governments abstained.

GUIDELINES GOVERNING THE PROTECTION OF PRIVACY  
AND TRANSBORDER FLOWS OF PERSONAL DATA

PART ONE. GENERAL

Definitions

1. For the purposes of these Guidelines:
  - (a) "data controller" means a party who, according to domestic law, is competent to decide about the contents and use of personal data regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf;
  - (b) "personal data" means any information relating to an identified or identifiable individual (data subject);
  - (c) "transborder flows of personal data" means movements of personal data across national borders.

Scope of Guidelines

2. These Guidelines apply to personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature or the context in which they are used, pose a danger to privacy and individual liberties.
3. These Guidelines should not be interpreted as preventing:
  - (a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;
  - (b) the exclusion from the application of the Guidelines of personal data which obviously do not contain any risk to privacy and individual liberties; or
  - (c) the application of the Guidelines only to automatic processing of personal data.
4. Exceptions to the Principles contained in Parts Two and Three of these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:
  - (a) as few as possible, and
  - (b) made known to the public.
5. In the particular case of Federal countries the observance of these Guidelines may be affected by the division of powers in the Federation.
6. These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.



## PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

### Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject:

### Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

### Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

### Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- (a) with the consent of the data subject; or
- (b) by the authority of law.

---

### Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

### Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

### Individual Participation Principle

13. An individual should have the right:
  - (a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

- (b) to have communicated to him, data relating to him
  - (i) within a reasonable time;
  - (ii) at a charge, if any, that is not excessive;
  - (iii) in a reasonable manner; and
  - (iv) in a form that is readily intelligible to him;
- (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
- (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, rectified, completed or amended.

#### Accountability Principle

- 14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

### PART THREE. BASIC PRINCIPLES OF INTERNATIONAL APPLICATION: FREE FLOW AND LEGITIMATE RESTRICTIONS

- 15. Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.
- 16. Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.
- 17. A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.
- 18. Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

#### PART FOUR. NATIONAL IMPLEMENTATION

19. In implementing domestically the principles set forth in Parts Two and Three, Member countries should establish legal, administrative or other procedures or institutions for the protection of privacy and individual liberties in respect of personal data. Member countries should in particular endeavour to:
- (a) adopt appropriate domestic legislation;
  - (b) encourage and support self-regulation, whether in the form of codes of conduct or otherwise;
  - (c) provide for reasonable means for individuals to exercise their rights;
  - (d) provide for adequate sanctions and remedies in case of failures to comply with measures which implement the principles set forth in Parts Two and Three; and
  - (e) ensure that there is no unfair discrimination against data subjects.

#### PART FIVE. INTERNATIONAL CO-OPERATION

20. Member countries should, where requested, make known to other Member countries details of the observance of the principles set forth in these Guidelines. Member countries should also ensure that procedures for transborder flows of personal data and for the protection of privacy and individual liberties are simple and compatible with those of other Member countries which comply with these Guidelines.
21. Member countries should establish procedures to facilitate:
- (i) information exchange related to these Guidelines, and
  - (ii) mutual assistance in the procedural and investigative matters involved.
22. Member countries should work towards the development of principles, domestic and international, to govern the applicable law in the case of transborder flows of personal data.

