OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

OECD

Includes the “Declaration on Transborder Data Flows” and the “Ministerial Declaration on the Protection of Privacy on Global Networks”.

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

Pursuant to Article 1 of the Convention signed in Paris on 14th December 1960, and which came into force on 30th September 1961, the Organisation for Economic Co-operation and Development (OECD) shall promote policies designed:

- to achieve the highest sustainable economic growth and employment and a rising standard of living in Member countries, while maintaining financial stability, and thus to contribute to the development of the world economy;
- to contribute to sound economic expansion in Member as well as non-member countries in the process of economic development; and
- to contribute to the expansion of world trade on a multilateral, non-discriminatory basis in accordance with international obligations.

The original Member countries of the OECD are Austria, Belgium, Canada, Denmark, France, Germany, Greece, Iceland, Ireland, Italy, Luxembourg, the Netherlands, Norway, Portugal, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The following countries became Members subsequently through accession at the dates indicated hereafter: Japan (28th April 1964), Finland (28th January 1969), Australia (7th June 1971), New Zealand (29th May 1973), Mexico (18th May 1994), the Czech Republic (21st December 1995), Hungary (7th May 1996), Poland (22nd November 1996), Korea (12th December 1996) and the Slovak Republic (14th December 2000). The Commission of the European Communities takes part in the work of the OECD (Article 13 of the OECD Convention).

Publié en français sous le titre :

Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel

FOREWORD

This publication contains the instruments that serve as the foundation for privacy protection at the global level: the 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the 1985 *Declaration on Transborder Data Flows* and the 1998 *Ministerial Declaration on the Protection of Privacy on Global Networks*. It is published on the responsibility of the Secretary-General of the OECD.

TABLE OF CONTENTS

PREFACE

With the introduction of information technology into various areas of economic and social life, and the growing importance and power of computerised data processing, the Organisation for Economic Co-operation and Development (OECD) decided, in 1980, to issue Guidelines on international policy on the protection of privacy and transborder flows of personal data.

More recently, the rapid and pervasive development of information and communications technologies and infrastructures, characterised by phenomena such as the Internet, has helped speed evolution towards a global information society. The OECD has therefore been focusing on how these Guidelines may best be implemented in the 21st century to help ensure respect of privacy and protection of personal data on line.

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980)

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (the "Privacy Guidelines") were adopted as a Recommendation of the OECD Council in support of the three principles that bind OECD Member countries: pluralistic democracy, respect for human rights and open market economies. They came into effect on 23 September 1980.

The Privacy Guidelines represent international consensus on general guidance concerning the collection and management of personal information. The principles set forth in the Privacy Guidelines are characterised by their clarity and flexibility of application and by their formulation, which is sufficiently broad to enable them to adapt to technological change. The principles encompass all media for the computerised processing of data on individuals (from local computers to networks with complex national and international ramifications), all types of personal data processing (from personnel administration to the compilation of consumer profiles) and all categories of data (from traffic data to content data, from the most mundane to the most sensitive). The principles are applicable at both national and international levels. Over the years, they have been put to use in a large number of national

regulatory or self-regulatory instruments and they are still widely used in both the public and private sectors.

Declaration on Transborder Data Flows (1985)

On 11 April 1985, OECD Ministers adopted the *Declaration on Transborder Data Flows*. This Declaration addressed the policy issues arising from flows of personal data across national borders, *e.g*. flows of data and information related to trading activities, intracorporate flows, computerised information services, and scientific and technological exchanges. In adopting this Declaration, OECD governments reaffirmed their commitment to developing common approaches to transborder data flow issues and, when appropriate, developing harmonised solutions. The *Declaration on Transborder Data Flows* is included in this publication.

Ministerial Declaration on the Protection of Privacy of Global Networks (1998)

More recently, at the OECD Ministerial level Conference "A Borderless World: Realising the Potential of Global Electronic Commerce", in Ottawa in 1998, Ministers reaffirmed "their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data." In particular, they declared that they would "work to build bridges between the different approaches adopted by Member countries to ensure privacy protection on global networks based on the OECD Privacy Guidelines." At the Conference, Ministers adopted a Declaration reaffirming their commitment to the protection of privacy on global networks, and launching action for future work in this area. The *Ministerial Declaration on the Protection of Privacy on Global Networks* is also included in this publication.

The 21st century

In the early part of this century, as accelerated technological change and globalisation create new challenges and opportunities for governments and citizens throughout the world, privacy is receiving increased attention and stands out as a fundamental social value. The OECD Member countries are fully committed to protecting privacy at the global level and are actively co-operating with business and industry, civil society, non-member countries and other international organisations to assess the key economic and technological trends that may have an impact on privacy, and develop comprehensive and consistent policies.

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

RECOMMENDATION OF THE COUNCIL
CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA

(23rd September, 1980)

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.

Annex to the Recommendation of the Council of 23rd September 1980

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.

EXPLANATORY MEMORANDUM

EXPLANATORY MEMORANDUM

INTRODUCTION

A feature of OECD Member countries over the past decade has been the development of laws for the protection of privacy. These laws have tended to assume different forms in different countries, and in many countries are still in the process of being developed. The disparities in legislation may create obstacles to the free flow of information between countries. Such flows have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology.

The OECD, which had been active in this field for some years past, decided to address the problems of diverging national legislation and in 1978 instructed a Group of Experts to develop Guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonisation of national legislation. The Group has now completed its work.

The Guidelines are broad in nature and reflect the debate and legislative work which has been going on for several years in Member countries. The Expert Group which prepared the Guidelines has considered it essential to issue an accompanying Explanatory Memorandum. Its purpose is to explain and elaborate the Guidelines and the basic problems of protection of privacy and individual liberties. It draws attention to key issues that have emerged in the discussion of the Guidelines and spells out the reasons for the choice of particular solutions.

The first part of the Memorandum provides general background information on the area of concern as perceived in Member countries. It explains the need for international action and summarises the work carried out so far by the OECD and certain other international organisations. It concludes with a list of the main problems encountered by the Expert Group in its work.

Part Two has two subsections. The first contains comments on certain general features of the Guidelines, the second detailed comments on individual paragraphs.

This Memorandum is an information document, prepared to explain and describe generally the work of the Expert Group. It is subordinate to the Guidelines themselves. It cannot vary the meaning of the Guidelines but is supplied to help in their interpretation and application.

I. GENERAL BACKGROUND

The problems

1. The 1970s may be described as a period of intensified investigative and legislative activities concerning the protection of privacy with respect to the collection and use of personal data. Numerous official reports show that the problems are taken seriously at the political level and at the same time that the task of balancing opposing interests is delicate and unlikely to be accomplished once and for all. Public interest has tended to focus on the risks and implications associated with the computerised processing of personal data and some countries have chosen to enact statutes which deal exclusively with computers and computer-supported activities. Other countries have preferred a more general approach to privacy protection issues irrespective of the particular data processing technology involved.

2. The remedies under discussion are principally safeguards for the individual which will prevent an invasion of privacy in the classical sense, *i.e*. abuse or disclosure of intimate personal data; but other, more or less closely related needs for protection have become apparent. Obligations of record-keepers to inform the general public about activities concerned with the processing of data, and rights of data subjects to have data relating to them supplemented or amended, are two random examples. Generally speaking, there has been a tendency to broaden the traditional concept of privacy ("the right to be left alone") and to identify a more complex synthesis of interests which can perhaps more correctly be termed privacy and individual liberties.

3. As far as the legal problems of automatic data processing (ADP) are concerned, the protection of privacy and individual liberties constitutes perhaps the most widely debated aspect. Among the reasons for such widespread concern are the ubiquitous use of computers for the processing of personal data, vastly expanded possibilities of storing, comparing, linking, selecting and accessing personal data, and the combination of computers and telecommunications technology which may place personal data simultaneously at the disposal of thousands of users at geographically dispersed locations and

enables the pooling of data and the creation of complex national and international data networks. Certain problems require particularly urgent attention, *e.g.* those relating to emerging international data networks, and to the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable.

Activities at national level

4. Of the OECD Member countries more than one-third have so far enacted one or several laws which, among other things, are intended to protect individuals against abuse of data relating to them and to give them the right of access to data with a view to checking their accuracy and appropriateness. In federal states, laws of this kind may be found both at the national and at the state or provincial level. Such laws are referred to differently in different countries. Thus, it is common practice in continental Europe to talk about "data laws" or "data protection laws" (*lois sur la protection des données*), whereas in English speaking countries they are usually known as "privacy protection laws". Most of the statutes were enacted after 1973 and this present period may be described as one of continued or even widened legislative activity. Countries which already have statutes in force are turning to new areas of protection or are engaged in revising or complementing existing statutes. Several other countries are entering the area and have bills pending or are studying the problems with a view to preparing legislation. These national efforts, and not least the extensive reports and research papers prepared by public committees or similar bodies, help to clarify the problems and the advantages and implications of various solutions. At the present stage, they provide a solid basis for international action.

5. The approaches to protection of privacy and individual liberties adopted by the various countries have many common features. Thus, it is possible to identify certain basic interests or values which are commonly considered to be elementary components of the area of protection. Some core principles of this type are: setting limits to the collection of personal data in accordance with the objectives of the data collector and similar criteria; restricting the usage of data to conform with openly specified purposes; creating facilities for individuals to learn of the existence and contents of data and have data corrected; and the identification of parties who are responsible for compliance with the relevant privacy protection rules and decisions. Generally speaking, statutes to protect privacy and individual liberties in relation to personal data attempt to cover the successive stages of the cycle beginning with

the initial collection of data and ending with erasure or similar measures, and to ensure to the greatest possible extent individual awareness, participation and control.

6. Differences between national approaches as apparent at present in laws, bills or proposals for legislation refer to aspects such as the scope of legislation, the emphasis placed on different elements of protection, the detailed implementation of the broad principles indicated above, and the machinery of enforcement. Thus, opinions vary with respect to licensing requirements and control mechanisms in the form of special supervisory bodies ("data inspection authorities"). Categories of sensitive data are defined differently, the means of ensuring openness and individual participation vary, to give just a few instances. Of course, existing traditional differences between legal systems are a cause of disparity, both with respect to legislative approaches and the detailed formulation of the regulatory framework for personal data protection.

International aspects of privacy and data banks

7. For a number of reasons the problems of developing safeguards for the individual in respect of the handling of personal data cannot be solved exclusively at the national level. The tremendous increase in data flows across national borders and the creation of international data banks (collections of data intended for retrieval and other purposes) have highlighted the need for concerted national action and at the same time support arguments in favour of free flows of information which must often be balanced against requirements for data protection and for restrictions on their collection, processing and dissemination.

8. One basic concern at the international level is for consensus on the fundamental principles on which protection of the individual must be based. Such a consensus would obviate or diminish reasons for regulating the export of data and facilitate resolving problems of conflict of laws. Moreover, it could constitute a first step towards the development of more detailed, binding international agreements.

9. There are other reasons why the regulation of the processing of personal data should be considered in an international context: the principles involved concern values which many nations are anxious to uphold and see generally accepted; they may help to save costs in international data traffic; countries have a common interest in preventing the creation of locations where national regulations on data processing can easily be circumvented; indeed, in view of the international mobility of people, goods and commercial and

scientific activities, commonly accepted practices with regard to the processing of data may be advantageous even where no transborder data traffic is directly involved.

Relevant international activities

10. There are several international agreements on various aspects of telecommunications which, while facilitating relations and co-operation between countries, recognise the sovereign right of each country to regulate its own telecommunications (The International Telecommunications Convention of 1973). The protection of computer data and programmes has been investigated by, among others, the World Intellectual Property Organisation which has developed draft model provisions for national laws on the protection of computer software. Specialised agreements aiming at informational co-operation may be found in a number of areas, such as law enforcement, health services, statistics and judicial services (*e.g.* with regard to the taking of evidence).

11. A number of international agreements deal in a more general way with the issues which are at present under discussion, viz. the protection of privacy and the free dissemination of information. They include the European Convention of Human Rights of 4th November, 1950 and the International Covenant on Civil and Political Rights (United Nations, 19th December, 1966).

12. However, in view of the inadequacy of existing international instruments relating to the processing of data and individual rights, a number of international organisations have carried out detailed studies of the problems involved in order to find more satisfactory solutions.

13. In 1973 and 1974 the Committee of Ministers of the ***Council of Europe*** adopted two resolutions concerning the protection of the privacy of individuals vis-à-vis electronic data banks in the private and public sectors respectively. Both resolutions recommend that the governments of the Member states of the Council of Europe take steps to give effect to a number of basic principles of protection relating to the obtaining of data, the quality of data, and the rights of individuals to be informed about data and data processing activities.

14. Subsequently the Council of Europe, on the instructions of its Committee of Ministers, began to prepare an international Convention on privacy protection in relation to data processing abroad and transfrontier data processing. It also initiated work on model regulations for medical data banks

and rules of conduct for data processing professionals. The Convention was adopted by the Committee of Ministers on 17th September 1980. It seeks to establish basic principles of data protection to be enforced by Member countries, to reduce restrictions on transborder data flows between the Contracting Parties on the basis of reciprocity, to bring about co-operation between national data protection authorities, and to set up a Consultative Committee for the application and continuing development of the convention.

15. The ***European Community*** has carried out studies concerning the problems of harmonisation of national legislations within the Community, in relation to transborder data flows and possible distortions of competition, the problems of data security and confidentiality, and the nature of transborder data flows. A sub-committee of the European Parliament held a public hearing on data processing and the rights of the individual in early 1978. Its work has resulted in a report to the European Parliament in spring 1979. The report, which was adopted by the European Parliament in May 1979, contains a resolution on the protection of the rights of the individual in the face of technical developments in data processing.

Activities of the OECD

16. The OECD programme on transborder data flows derives from computer utilisation studies in the public sector which were initiated in 1969. A Group of Experts, the Data Bank Panel, analysed and studied different aspects of the privacy issue, *e.g.* in relation to digital information, public administration, transborder data flows, and policy implications in general. In order to obtain evidence on the nature of the problems, the Data Bank Panel organised a Symposium in Vienna in 1977 which provided opinions and experience from a diversity of interests, including government, industry, users of international data communication networks, processing services, and interested intergovernmental organisations.

17. A number of guiding principles were elaborated in a general framework for possible international action. These principles recognised (a) the need for generally continuous and uninterrupted flows of information between countries, (b) the legitimate interests of countries in preventing transfers of data which are dangerous to their security or contrary to their laws on public order and decency or which violate the rights of their citizens, (c) the economic value of information and the importance of protecting “data trade” by accepted rules of fair competition, (d) the needs for security safeguards to minimise violations of proprietary data and misuse of personal information, and (e) the significance

of a commitment of countries to a set of core principles for the protection of personal information.

18. Early in 1978 a new ad hoc Group of Experts on Transborder Data Barriers and Privacy Protection was set up within the OECD which was instructed to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate a harmonisation of national legislations, without this precluding at a later date the establishment of an international Convention. This work was to be carried out in close co-operation with the Council of Europe and the European Community and to be completed by lst July 1979.

19. The Expert Group, under the chairmanship of the Honourable Mr. Justice Kirby, Australia, and with the assistance of Dr. Peter Seipel (Consultant), produced several drafts and discussed various reports containing, for instance, comparative analyses of different approaches to legislation in this field. It was particularly concerned with a number of key issues set out below.

a) The specific, sensitive facts issue

The question arose as to whether the Guidelines should be of a general nature or whether they should be structured to deal with different types of data or activities (*e.g.* credit reporting). Indeed, it is probably not possible to identify a set of data which are universally regarded as being sensitive.

b) The ADP issue

The argument that ADP is the main cause for concern is doubtful and, indeed, contested.

c) The legal persons issue

Some, but by no means all, national laws protect data relating to legal persons in a similar manner to data related to physical persons.

d) The remedies and sanctions issue

The approaches to control mechanisms vary considerably: for instance, schemes involving supervision and licensing by specially constituted authorities might be

compared to schemes involving voluntary compliance by record-keepers and reliance on traditional judicial remedies in the Courts.

e) The basic machinery or implementation issue

The choice of core principles and their appropriate level of detail presents difficulties. For instance, the extent to which data security questions (protection of data against unauthorised interference, fire, and similar occurrences) should be regarded as part of the privacy protection complex is debatable; opinions may differ with regard to time limits for the retention, or requirements for the erasure, of data and the same applies to requirements that data be relevant to specific purposes. In particular, it is difficult to draw a clear dividing line between the level of basic principles or objectives and lower level "machinery" questions which should be left to domestic implementation.

f) The choice of law issue

The problems of choice of jurisdiction, choice of applicable law and recognition of foreign judgements have proved to be complex in the context of transborder data flows. The question arose, however, whether and to what extent it should be attempted at this stage to put forward solutions in Guidelines of a non-binding nature.

g) The exceptions issue

Similarly, opinions may vary on the question of exceptions. Are they required at all? If so, should particular categories of exceptions be provided for or should general limits to exceptions be formulated?

h) The bias issue

Finally, there is an inherent conflict between the protection and the free transborder flow of personal data. Emphasis may be placed on one or the other, and interests in privacy protection may be difficult to distinguish from other interests relating to trade, culture, national sovereignty, and so forth.

20. During its work the Expert Group maintained close contacts with corresponding organs of the Council of Europe. Every effort was made to avoid unnecessary differences between the texts produced by the two organisations;

thus, the set of basic principles of protection are in many respects similar. On the other hand, a number of differences do occur. To begin with, the OECD Guidelines are not legally binding, whereas the Council of Europe has produced a convention which will be legally binding among those countries which ratify it. This in turn means that the question of exceptions has been dealt with in greater detail by the Council of Europe. As for the area of application, the Council of Europe Convention deals primarily with the automatic processing of personal data whereas the OECD Guidelines apply to personal data which involve dangers to privacy and individual liberties, irrespective of the methods and machinery used in their handling. At the level of details, the basic principles of protection proposed by the two organisations are not identical and the terminology employed differs in some respects. The institutional framework for continued co-operation is treated in greater detail in the Council of Europe Convention than in the OECD Guidelines.

21. The Expert Group also maintained co-operation with the Commission of the European Communities as required by its mandate.

II. THE GUIDELINES

A. PURPOSE AND SCOPE

General

22. The Preamble of the Recommendation expresses the basic concerns calling for action. The Recommendation affirms the commitment of Member countries to protect privacy and individual liberties and to respect the transborder flows of personal data.

23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7-14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, *i.e.* principles which are chiefly concerned with relationships between Member countries.

24. Part Four deals, in general terms, with means of implementing the basic principles set out in the preceding parts and specifies that these principles should be applied in a non-discriminatory manner. Part Five concerns matters of mutual assistance between Member countries, chiefly through the exchange of information and by avoiding incompatible national procedures for the protection of personal data. It concludes with a reference to issues of applicable law which may arise when flows of personal data involve several Member countries.

Objectives

25. The core of the Guidelines consists of the principles set out in Part Two of the Annex. It is recommended to Member countries that they adhere to these principles with a view to:

a) achieving acceptance by Member countries of certain minimum standards of protection of privacy and individual liberties with regard to personal data;

b) reducing differences between relevant domestic rules and practices of Member countries to a minimum;

c) ensuring that in protecting personal data they take into consideration the interests of other Member countries and the need to avoid undue interference with flows of personal data between Member countries; and

d) eliminating, as far as possible, reasons which might induce Member countries to restrict transborder flows of personal data because of the possible risks associated with such flows.

As stated in the Preamble, two essential basic values are involved: the protection of privacy and individual liberties and the advancement of free flows of personal data. The Guidelines attempt to balance the two values against one another; while accepting certain restrictions to free transborder flows of personal data, they seek to reduce the need for such restrictions and thereby strengthen the notion of free information flows between countries.

26. Finally, Parts Four and Five of the Guidelines contain principles seeking to ensure:

a) effective national measures for the protection of privacy and individual liberties;

b) avoidance of practices involving unfair discrimination between individuals; and

c) bases for continued international co-operation and compatible procedures in any regulation of transborder flows of personal data.

Level of detail

27. The level of detail of the Guidelines varies depending upon two main factors, viz. (a) the extent of consensus reached concerning the solutions put forward, and (b) available knowledge and experience pointing to solutions to be adopted at this stage. For instance, the Individual Participation Principle (Paragraph 13) deals specifically with various aspects of protecting an individual's interest, whereas the provision on problems of choice of law and related matters (Paragraph 22) merely states a starting-point for a gradual development of detailed common approaches and international agreements. On the whole, the Guidelines constitute a general framework for concerted actions by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation. To conclude, there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly.

Non-member countries

28. The Recommendation is addressed to Member countries and this is reflected in several provisions which are expressly restricted to relationships between Member countries (see Paragraphs 15, 17 and 20 of the Guidelines). Widespread recognition of the Guidelines is, however, desirable and nothing in them should be interpreted as preventing the application of relevant provisions by Member countries to non-member countries. In view of the increase in transborder data flows and the need to ensure concerted solutions, efforts will be made to bring the Guidelines to the attention of non-member countries and appropriate international organisations.

The broader regulatory perspective

29. It has been pointed out earlier that the protection of privacy and individual liberties constitutes one of many overlapping legal aspects involved in the processing of data. The Guidelines constitute a new instrument, in addition to other, related international instruments governing such issues as human rights, telecommunications, international trade, copyright, and various information services. If the need arises, the principles set out in the Guidelines could be further developed within the framework of activities undertaken by the OECD in the area of information, computer and communications policies.

30. Some Member countries have emphasised the advantages of a binding international Convention with a broad coverage. The Mandate of the Expert Group required it to develop guidelines on basic rules governing the transborder flow and the protection of personal data and privacy, without this precluding at a later stage the establishment of an international Convention of a binding nature. The Guidelines could serve as a starting-point for the development of an international Convention when the need arises.

Legal persons, groups and similar entities

31. Some countries consider that the protection required for data relating to individuals may be similar in nature to the protection required for data relating to business enterprises, associations and groups which may or may not possess legal personality. The experience of a number of countries also shows that it is difficult to define clearly the dividing line between personal and non-personal data. For example, data relating to a small company may also concern its owner or owners and provide personal information of a more or less sensitive nature. In such instances it may be advisable to extend to corporate entities the protection offered by rules relating primarily to personal data.

32. Similarly, it is debatable to what extent people belonging to a particular group (*i.e.* mentally disabled persons, immigrants, ethnic minorities) need additional protection against the dissemination of information relating to that group.

33. On the other hand, the Guidelines reflect the view that the notions of individual integrity and privacy are in many respects particular and should not be treated the same way as the integrity of a group of persons, or corporate security and confidentiality. The needs for protection are different and so are the policy frameworks within which solutions have to be formulated and interests balanced against one another. Some members of the Expert Group suggested that the possibility of extending the Guidelines to legal persons (corporations, associations) should be provided for. This suggestion has not secured a sufficient consensus. The scope of the Guidelines is therefore confined to data relating to individuals and it is left to Member countries to draw dividing lines and decide policies with regard to corporations, groups and similar bodies (*cf.* paragraph 49 below).

Automated and non-automated data

34. In the past, OECD activities in privacy protection and related fields have focused on automatic data processing and computer networks. The Expert Group has devoted special attention to the issue of whether or not these Guidelines should be restricted to the automatic and computer-assisted processing of personal data. Such an approach may be defended on a number of grounds, such as the particular dangers to individual privacy raised by automation and computerised data banks, and increasing dominance of automatic data processing methods, especially in transborder data flows, and the particular framework of information, computer and communications policies within which the Expert Group has set out to fulfil its Mandate.

35. On the other hand, it is the conclusion of the Expert Group that limiting the Guidelines to the automatic processing of personal data would have considerable drawbacks. To begin with, it is difficult, at the level of definitions, to make a clear distinction between the automatic and non-automatic handling of data. There are, for instance, "mixed" data processing systems, and there are stages in the processing of data which may or may not lead to automatic treatment. These difficulties tend to be further complicated by ongoing technological developments, such as the introduction of advanced semi-automated methods based on the use of microfilm, or microcomputers which may increasingly be used for private purposes that are both harmless and impossible to control. Moreover, by concentrating exclusively on computers the Guidelines might lead to inconsistency and lacunae, and opportunities for record-keepers to circumvent rules which implement the Guidelines by using non-automatic means for purposes which may be offensive.

36. Because of the difficulties mentioned, the Guidelines do not put forward a definition of "automatic data processing" although the concept is referred to in the preamble and in paragraph 3 of the Annex. It may be assumed that guidance for the interpretation of the concept can be obtained from sources such as standard technical vocabularies.

37. Above all, the principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed. The Guidelines therefore apply to personal data in general or, more precisely, to personal data which, because of the manner in which they are processed, or because of their nature or context, pose a danger to privacy and individual liberties.

38. It should be noted, however, that the Guidelines do not constitute a set of general privacy protection principles; invasions of privacy by, for instance,

candid photography, physical maltreatment, or defamation are outside their scope unless such acts are in one way or another associated with the handling of personal data. Thus, the Guidelines deal with the building-up and use of aggregates of data which are organised for retrieval, decision-making, research, surveys and similar purposes. It should be emphasised that the Guidelines are neutral with regard to the particular technology used; automatic methods are only one of the problems raised in the Guidelines although, particularly in the context of transborder data flows, this is clearly an important one.

B. DETAILED COMMENTS

General

39. The comments which follow relate to the actual Guidelines set out in the Annex to the Recommendation. They seek to clarify the debate in the Expert Group.

Paragraph 1: Definitions

40. The list of definitions has been kept short. The term ***"data controller"*** is of vital importance. It attempts to define a subject who, under domestic law, should carry ultimate responsibility for activities concerned with the processing of personal data. As defined, the data controller is a party who is legally competent to decide about the contents and use of data, regardless of whether or not such data are collected, stored, processed or disseminated by that party or by an agent on its behalf. The data controller may be a legal or natural person, public authority, agency or any other body. The definition excludes at least four categories which may be involved in the processing of data, viz. (a) licensing authorities and similar bodies which exist in some Member countries and which authorise the processing of data but are not entitled to decide (in the proper sense of the word) what activities should be carried out and for what purposes; (b) data processing service bureaux which carry out data processing on behalf of others; (c) telecommunications authorities and similar bodies which act as mere conduits; and (d) "dependent users" who may have access to data but who are not authorised to decide what data should be stored, who should be able to use them, etc. In implementing the Guidelines, countries may develop more complex schemes of levels and types of responsibilities. Paragraphs 14 and 19 of the Guidelines provide a basis for efforts in this direction.

41. The terms "***personal data***" and "***data subject***" serve to underscore that the Guidelines are concerned with physical persons. The precise dividing line between personal data in the sense of information relating to identified or identifiable individuals and anonymous data may be difficult to draw and must be left to the regulation of each Member country. In principle, personal data convey information which by direct (*e.g.* a civil registration number) or indirect linkages (*e.g.* an address) may be connected to a particular physical person.

42. The term "***transborder flows of personal data***" restricts the application of certain provisions of the Guidelines to international data flows and consequently omits the data flow problems particular to federal states. The movements of data will often take place through electronic transmission but other means of data communication may also be involved. Transborder flows as understood in the Guidelines includes the transmission of data by satellite.

Paragraph 2: Area of application

43. The Section of the Memorandum dealing with the scope and purpose of the Guidelines introduces the issue of their application to the automatic as against non-automatic processing of personal data. Paragraph 2 of the Guidelines, which deals with this problem, is based on two limiting criteria. The first is associated with the concept of personal data: the Guidelines apply to data which can be related to identified or identifiable individuals. Collections of data which do not offer such possibilities (collections of statistical data in anonymous form) are not included. The second criterion is more complex and relates to a specific risk element of a factual nature, viz. that data pose a danger to privacy and individual liberties. Such dangers can arise because of the use of automated data processing methods (the manner in which data are processed), but a broad variety of other possible risk sources is implied. Thus, data which are in themselves simple and factual may be used in a context where they become offensive to a data subject. On the other hand, the risks as expressed in Paragraph 2 of the Guidelines are intended to exclude data collections of an obviously innocent nature (*e.g.* personal notebooks). The dangers referred to in Paragraph 2 of the Guidelines should relate to privacy and individual liberties. However, the protected interests are broad (cf. paragraph 2 above) and may be viewed differently by different Member countries and at different times. A delimitation as far as the Guidelines are concerned and a common basic approach are provided by the principles set out in Paragraphs 7 to 13.

44. As explained in Paragraph 2 of the Guidelines, they are intended to cover both the private and the public sector. These notions may be defined differently by different Member countries.

Paragraph 3: Different degrees of sensitivity

45. The Guidelines should not be applied in a mechanistic way irrespective of the kind of data and processing activities involved. The framework provided by the basic principles in Part Two of the Guidelines permits Member countries to exercise their discretion with respect to the degree of stringency with which the Guidelines are to be implemented, and with respect to the scope of the measures to be taken. In particular, Paragraph 3(b) provides for many "trivial" cases of collection and use of personal data (cf. above) to be completely excluded from the application of the Guidelines. Obviously this does not mean that Paragraph 3 should be regarded as a vehicle for demolishing the standards set up by the Guidelines. But, generally speaking, the Guidelines do not presuppose their uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account. Thus, in one country universal personal identifiers may be considered both harmless and useful whereas in another country they may be regarded as highly sensitive and their use restricted or even forbidden. In one country, protection may be afforded to data relating to groups and similar entities whereas such protection is completely non-existent in another country, and so forth. To conclude, some Member countries may find it appropriate to restrict the application of the Guidelines to the automatic processing of personal data. Paragraph 3(c) provides for such a limitation.

Paragraph 4: Exceptions to the Guidelines

46. To provide formally for exceptions in Guidelines which are part of a non-binding Recommendation may seem superfluous. However, the Expert Group has found it appropriate to include a provision dealing with this subject and stating that two general criteria ought to guide national policies in limiting the application of the Guidelines: exceptions should be as few as possible, and they should be made known to the public (*e.g.* through publication in an official government gazette). General knowledge of the existence of certain data or files would be sufficient to meet the second criterion, although details concerning particular data etc. may have to be kept secret. The formula provided in Paragraph 4 is intended to cover many different kinds of concerns and limiting factors, as it was obviously not possible to provide an exhaustive list of exceptions – hence the wording that they include national sovereignty, national security and public policy (*"ordre public"*). Another overriding national concern would be, for instance, the financial interests of the State (*"crédit public"*). Moreover, Paragraph 4 allows for different ways of implementing the Guidelines: it should be borne in mind that Member countries are at present at

different stages of development with respect to privacy protection rules and institutions and will probably proceed at different paces, applying different strategies, *e.g.* the regulation of certain types of data or activities as compared to regulation of a general nature ("omnibus approach").

47. The Expert Group recognised that Member countries might apply the Guidelines differentially to different kinds of personal data. There may be differences in the permissible frequency of inspection, in ways of balancing competing interests such as the confidentiality of medical records versus the individual's right to inspect data relating to him, and so forth. Some examples of areas which may be treated differently are credit reporting, criminal investigation and banking. Member countries may also choose different solutions with respect to exceptions associated with, for example, research and statistics. An exhaustive enumeration of all such situations and concerns is neither required nor possible. Some of the subsequent paragraphs of the Guidelines and the comments referring to them provide further clarification of the area of application of the Guidelines and of the closely related issues of balancing opposing interests (compare with Paragraphs 7, 8, 17 and 18 of the Guidelines). To summarise, the Expert Group has assumed that exceptions will be limited to those which are necessary in a democratic society.

Paragraph 5: Federal countries

48. In Federal countries, the application of the Guidelines is subject to various constitutional limitations. Paragraph 5, accordingly, serves to underscore that no commitments exist to apply the Guidelines beyond the limits of constitutional competence.

Paragraph 6: Minimum standards

49. First, Paragraph 6 describes the Guidelines as minimum standards for adoption in domestic legislation. Secondly, and in consequence, it has been agreed that the Guidelines are capable of being supplemented by additional measures for the protection of privacy and individual liberties at the national as well as the international level.

Paragraph 7: Collection Limitation Principle

50. As an introductory comment on the principles set out in Paragraphs 7 to 14 of the Guidelines it should be pointed out that these principles are

interrelated and partly overlapping. Thus, the distinctions between different activities and stages involved in the processing of data which are assumed in the principles, are somewhat artificial and it is essential that the principles are treated together and studied as a whole. Paragraph 7 deals with two issues, viz. (a) limits to the collection of data which, because of the manner in which they are to be processed, their nature, the context in which they are to be used or other circumstances, are regarded as specially sensitive; and (b) requirements concerning data collection methods. Different views are frequently put forward with respect to the first issue. It could be argued that it is both possible and desirable to enumerate types or categories of data which are per se sensitive and the collection of which should be restricted or even prohibited. There are precedents in European legislation to this effect (race, religious beliefs, criminal records, for instance). On the other hand, it may be held that no data are intrinsically "private" or "sensitive" but may become so in view of their context and use. This view is reflected, for example, in the privacy legislation of the United States.

51. The Expert Group discussed a number of sensitivity criteria, such as the risk of discrimination, but has not found it possible to define any set of data which are universally regarded as sensitive. Consequently, Paragraph 7 merely contains a general statement that there should be limits to the collection of personal data. For one thing, this represents an affirmative recommendation to lawmakers to decide on limits which would put an end to the indiscriminate collection of personal data. The nature of the limits is not spelt out but it is understood that the limits may relate to:

- data quality aspects (*i.e.* that it should be possible to derive information of sufficiently high quality from the data collected, that data should be collected in a proper information framework, etc.);

- limits associated with the purpose of the processing of data (*i.e.* that only certain categories of data ought to be collected and, possibly, that data collection should be restricted to the minimum necessary to fulfil the specified purpose);

- "earmarking" of specially sensitive data according to traditions and attitudes in each Member country;

- limits to data collection activities of certain data controllers;

- civil rights concerns.

52. The second part of Paragraph 7 (data collection methods) is directed against practices which involve, for instance, the use of hidden data registration devices such as tape recorders, or deceiving data subjects to make them supply information. The knowledge or consent of the data subject is as a rule essential, knowledge being the minimum requirement. On the other hand, consent cannot always be imposed, for practical reasons. In addition, Paragraph 7 contains a reminder ("where appropriate") that there are situations where for practical or policy reasons the data subject's knowledge or consent cannot be considered necessary. Criminal investigation activities and the routine up-dating of mailing lists may be mentioned as examples. Finally, Paragraph 7 does not exclude the possibility of a data subject being represented by another party, for instance in the case of minors, mentally disabled person, etc.

Paragraph 8: Data Quality Principle

53. Requirements that data be relevant can be viewed in different ways. In fact, some members of the Expert Group hesitated as to whether such requirements actually fitted into the framework of privacy protection. The conclusion of the Group was to the effect, however, that data should be related to the purpose for which they are to be used. For instance, data concerning opinions may easily be misleading if they are used for purposes to which they bear no relation, and the same is true of evaluative data. Paragraph 8 also deals with accuracy, completeness and up-to-dateness which are all important elements of the data quality concept. The requirements in this respect are linked to the purposes of data, *i.e.* they are not intended to be more far-reaching than is necessary for the purposes for which the data are used. Thus, historical data may often have to be collected or retained; cases in point are social research, involving so-called longitudinal studies of developments in society, historical research, and the activities of archives. The "purpose test" will often involve the problem of whether or not harm can be caused to data subjects because of lack of accuracy, completeness and up-dating.

Paragraph 9: Purpose Specification Principle

54. The Purpose Specification Principle is closely associated with the two surrounding principles, *i.e.* the Data Quality Principle and the Use Limitation Principle. Basically, Paragraph 9 implies that before, and in any case not later than at the time data collection it should be possible to identify the purposes for which these data are to be used, and that later changes of purposes should likewise be specified. Such specification of purposes can be made in a number of alternative or complementary ways, *e.g.* by public declarations, information

to data subjects, legislation, administrative decrees, and licences provided by supervisory bodies. According to Paragraphs 9 and 10, new purposes should not be introduced arbitrarily; freedom to make changes should imply compatibility with the original purposes. Finally, when data no longer serve a purpose, and if it is practicable, it may be necessary to have them destroyed (erased) or given an anonymous form. The reason is that control over data may be lost when data are no longer of interest; this may lead to risks of theft, unauthorised copying or the like.

Paragraph 10: Use Limitation Principle

55. This paragraph deals with uses of different kinds, including disclosure, which involve deviations from specified purposes. For instance, data may be transmitted from one computer to another where they can be used for unauthorised purposes without being inspected and thus disclosed in the proper sense of the word. As a rule the initially or subsequently specified purposes should be decisive for the uses to which data can be put. Paragraph 10 foresees two general exceptions to this principle: the consent of the data subject (or his representative – see Paragraph 52 above) and the authority of law (including, for example, licences granted by supervisory bodies). For instance, it may be provided that data which have been collected for purposes of administrative decision-making may be made available for research, statistics and social planning.

Paragraph 11: Security Safeguards Principle

56. Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasised that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. Paragraph 11 has a broad coverage. The cases mentioned in the provision are to some extent overlapping (*e.g.* access/ disclosure). “Loss” of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. “Modified” should be construed to cover unauthorised input of data, and “use” to cover unauthorised copying.

Paragraph 12: Openness Principle

57. The Openness Principle may be viewed as a prerequisite for the Individual Participation Principle (Paragraph 13); for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data. Regular information from data controllers on a voluntary basis, publication in official registers of descriptions of activities concerned with the processing of personal data, and registration with public bodies are some, though not all, of the ways by which this may be brought about. The reference to means which are "readily available" implies that individuals should be able to obtain information without unreasonable effort as to time, advance knowledge, travelling, and so forth, and without unreasonable cost.

Paragraph 13: Individual Participation Principle

58. The right of individuals to access and challenge personal data is generally regarded as perhaps the most important privacy protection safeguard. This view is shared by the Expert Group which, although aware that the right to access and challenge cannot be absolute, has chosen to express it in clear and fairly specific language. With respect to the individual sub-paragraphs, the following explanations are called for:

59. The right to access should as a rule be simple to exercise. This may mean, among other things, that it should be part of the day-to-day activities of the data controller or his representative and should not involve any legal process or similar measures. In some cases it may be appropriate to provide for intermediate access to data; for example, in the medical area a medical practitioner can serve as a go-between. In some countries supervisory organs, such as data inspection authorities, may provide similar services. The requirement that data be communicated within reasonable time may be satisfied in different ways. For instance, a data controller who provides information to data subjects at regular intervals may be exempted from obligations to respond at once to individual requests. Normally, the time is to be counted from the receipt of a request. Its length may vary to some extent from one situation to another depending on circumstances such as the nature of the data processing activity. Communication of such data "in a reasonable manner" means, among other things, that problems of geographical distance should be given due attention. Moreover, if intervals are prescribed between the times when requests for access must be met, such intervals should be reasonable. The extent to which data subjects should be able to obtain copies of data relating to them is a

matter of implementation which must be left to the decision of each Member country.

60. The right to reasons in Paragraph 13(c) is narrow in the sense that it is limited to situations where requests for information have been refused. A broadening of this right to include reasons for adverse decisions in general, based on the use of personal data, met with sympathy in the Expert Group. However, on final consideration a right of this kind was thought to be too broad for insertion in the privacy framework constituted by the Guidelines. This is not to say that a right to reasons for adverse decisions may not be appropriate, *e.g.* in order to inform and alert a subject to his rights so that he can exercise them effectively.

61. The right to challenge in 13(c) and (d) is broad in scope and includes first instance challenges to data controllers as well as subsequent challenges in courts, administrative bodies, professional organs or other institutions according to domestic rules of procedure (compare with Paragraph 19 of the Guidelines). The right to challenge does not imply that the data subject can decide what remedy or relief is available (rectification, annotation that data are in dispute, etc.): such matters will be decided by domestic law and legal procedures. Generally speaking, the criteria which decide the outcome of a challenge are those which are stated elsewhere in the Guidelines.

Paragraph 14: Accountability Principle

62. The data controller decides about data and data processing activities. It is for his benefit that the processing of data is carried out. Accordingly. it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau. On the other hand, nothing in the Guidelines prevents service bureaux personnel, "dependent users" (see paragraph 40) and others from also being held accountable. For instance, sanctions against breaches of confidentiality obligations may be directed against all parties entrusted with the handling of personal information (*cf.* Paragraph 19 of the Guidelines). Accountability under Paragraph 14 refers to accountability supported by legal sanctions, as well as to accountability established by codes of conduct, for instance.

Paragraphs 15-18: Basic Principles of International Application

63. The principles of international application are closely interrelated. Generally speaking, Paragraph 15 concerns respect by Member countries for each other's interest in protecting personal data, and the privacy and individual liberties of their nationals and residents. Paragraph 16 deals with security issues in a broad sense and may be said to correspond, at the international level, to Paragraph 11 of the Guidelines. Paragraphs 17 and 18 deal with restrictions on free flows of personal data between Member countries; basically, as far as protection of privacy and individual liberties is concerned, such flows should be admitted as soon as requirements of the Guidelines for the protection of these interests have been substantially, *i.e.* effectively, fulfilled. The question of other possible bases of restricting transborder flows of personal data is not dealt with in the Guidelines.

64. For domestic processing **Paragraph 15** has two implications. First, it is directed against liberal policies which are contrary to the spirit of the Guidelines and which facilitate attempts to circumvent or violate protective legislation of other Member countries. However, such circumvention or violation, although condemned by all Member countries, is not specifically mentioned in this Paragraph as a number of countries felt it to be unacceptable that one Member country should be required to directly or indirectly enforce, extraterritorially, the laws of other Member countries. It should be noted that the provision explicitly mentions the re-export of personal data. In this respect, Member countries should bear in mind the need to support each other's efforts to ensure that personal data are not deprived of protection as a result of their transfer to territories and facilities for the processing of data where control is slack or non-existent.

65. Secondly, Member countries are implicitly encouraged to consider the need to adapt rules and practices for the processing of data to the particular circumstances which may arise when foreign data and data on non-nationals are involved. By way of illustration, a situation may arise where data on foreign nationals are made available for purposes which serve the particular interests of their country of nationality (*e.g.* access to the addresses of nationals living abroad).

66. As far as the Guidelines are concerned, the encouragement of international flows of personal data is not an undisputed goal in itself. To the extent that such flows take place they should, however, according to **Paragraph 16**, be uninterrupted and secure, *i.e.* protected against unauthorised access, loss of data and similar events. Such protection should also be given to data in transit, *i.e.* data which pass through a Member country without being

used or stored with a view to usage in that country. The general commitment under Paragraph 16 should, as far as computer networks are concerned, be viewed against the background of the International Telecommunications Convention of Malaga-Torremolinos (25th October, 1973). According to that convention, the members of the International Telecommunications Union, including the OECD Member countries, have agreed, *inter alia*, to ensure the establishment, under the best technical conditions, of the channels and installations necessary to carry on the rapid and uninterrupted exchange of international telecommunications. Moreover, the members of ITU have agreed to take all possible measures compatible with the telecommunications system used to ensure the secrecy of international correspondence. As regards exceptions, the right to suspend international telecommunications services has been reserved and so has the right to communicate international correspondence to the competent authorities in order to ensure the application of internal laws or the execution of international conventions to which members of the ITU are parties. These provisions apply as long as data move through telecommunications lines. In their context, the Guidelines constitute a complementary safeguard that international flows of personal data should be uninterrupted and secure.

67. **Paragraph 17** reinforces Paragraph 16 as far as relationships between Member countries are concerned. It deals with interests which are opposed to free transborder flows of personal data but which may nevertheless constitute legitimate grounds for restricting such flows between Member countries. A typical example would be attempts to circumvent national legislation by processing data in a Member country which does not yet substantially observe the Guidelines. Paragraph 17 establishes a standard of equivalent protection, by which is meant protection which is substantially similar in effect to that of the exporting country, but which need not be identical in form or in all respects. As in Paragraph 15, the re-export of personal data is specifically mentioned – in this case with a view to preventing attempts to circumvent the domestic privacy legislation of Member countries. The third category of grounds for legitimate restrictions mentioned in Paragraph 17, concerning personal data of a special nature, covers situations where important interests of Member countries could be affected. Generally speaking, however, paragraph 17 is subject to Paragraph 4 of the Guidelines which implies that restrictions on flows of personal data should be kept to a minimum.

68. **Paragraph 18** attempts to ensure that privacy protection interests are balanced against interests of free transborder flows of personal data. It is directed in the first place against the creation of barriers to flows of personal data which are artificial from the point of view of protection of privacy and individual liberties and fulfil restrictive purposes of other kinds which are thus

not openly announced. However, Paragraph 18 is not intended to limit the rights of Member countries to regulate transborder flows of personal data in areas relating to free trade, tariffs, employment, and related economic conditions for intentional data traffic. These are matters which were not addressed by the Expert Group, being outside its Mandate.

Paragraph 19: National Implementation

69. The detailed implementation of Parts Two and Three of the Guidelines is left in the first place to Member countries. It is bound to vary according to different legal systems and traditions, and Paragraph 19 therefore attempts merely to establish a general framework indicating in broad terms what kind of national machinery is envisaged for putting the Guidelines into effect. The opening sentence shows the different approaches which might be taken by countries, both generally and with respect to control mechanisms (*e.g.* specially set up supervisory bodies, existing control facilities such as courts, public authorities, etc.).

70. In Paragraph 19(a) countries are invited to adopt appropriate domestic legislation, the word "appropriate" foreshadowing the judgement by individual countries of the appropriateness or otherwise of legislative solutions. Paragraph 19(b) concerning self-regulation is addressed primarily to common law countries where non-legislative implementation of the Guidelines would complement legislative action. Paragraph 19(c) should be given a broad interpretation; it includes such means as advice from data controllers and the provision of assistance, including legal aid. Paragraph 19(d) permits different approaches to the issue of control mechanisms: briefly, either the setting-up of special supervisory bodies, or reliance on already existing control facilities, whether in the form of courts, existing public authorities or otherwise. Paragraph 19(e) dealing with discrimination is directed against unfair practices but leaves open the possibility of "benign discrimination" to support disadvantaged groups, for instance. The provision is directed against unfair discrimination on such bases as nationality and domicile, sex, race, creed, or trade union affiliation.

Paragraph 20: Information Exchange and Compatible Procedures

71. Two major problems are dealt with here, viz. (a) the need to ensure that information can be obtained about rules, regulations, decisions, etc., which implement the Guidelines, and (b) the need to avoid transborder flows of personal data being hampered by an unnecessarily complex and disparate

framework of procedures and compliance requirements. The first problem arises because of the complexity of privacy protection regulation and data policies in general. There are often several levels of regulation (in a broad sense) and many important rules cannot be laid down permanently in detailed statutory provisions; they have to be kept fairly open and left to the discretion of lower-level decision-making bodies.

72. The importance of the second problem is, generally speaking, proportional to the number of domestic laws which affect transborder flows of personal data. Even at the present stage, there are obvious needs for co-ordinating special provisions on transborder data flows in domestic laws, including special arrangements relating to compliance control and, where required, licences to operate data processing systems.

Paragraph 21: Machinery for Co-operation

73. The provision on national procedures assumes that the Guidelines will form a basis for continued co-operation. Data protection authorities and specialised bodies dealing with policy issues in information and data communications are obvious partners in such a co-operation. In particular, the second purpose of such measures, contained in Paragraph 21(ii), *i.e.* mutual aid in procedural matters and requests for information, is future-oriented: its practical significance is likely to grow as international data networks and the complications associated with them become more numerous.

Paragraph 22: Conflicts of Laws

74. The Expert Group has devoted considerable attention to issues of conflicts of laws, and in the first place to the questions as to which courts should have jurisdiction over specific issues (choice of jurisdiction) and which system of law should govern specific issues (choice of law). The discussion of different strategies and proposed principles has confirmed the view that at the present stage, with the advent of such rapid changes in technology, and given the non-binding nature of the Guidelines, no attempt should be made to put forward specific, detailed solutions. Difficulties are bound to arise with respect to both the choice of a theoretically sound regulatory model and the need for additional experience about the implications of solutions which in themselves are possible.

75. As regards the question of choice of law, one way of approaching these problems is to identify one or more connecting factors which, at best,

indicate one applicable law. This is particularly difficult in the case of international computer networks where, because of dispersed location and rapid movement of data, and geographically dispersed data processing activities, several connecting factors could occur in a complex manner involving elements of legal novelty. Moreover, it is not evident what value should presently be attributed to rules which by mechanistic application establish the specific national law to be applied. For one thing, the appropriateness of such a solution seems to depend upon the existence of both similar legal concepts and rule structures, and binding commitments of nations to observe certain standards of personal data protection. In the absence of these conditions, an attempt could be made to formulate more flexible principles which involve a search for a "proper law" and are linked to the purpose of ensuring effective protection of privacy and individual liberties. Thus, in a situation where several laws may be applicable, it has been suggested that one solution could be to give preference to the domestic law offering the best protection of personal data. On the other hand, it may be argued that solutions of this kind leave too much uncertainty, not least from the point of view of the data controllers who may wish to know, where necessary in advance, by which national systems of rules an international data processing system will be governed.

76. In view of these difficulties, and considering that problems of conflicts of laws might best be handled within the total framework of personal and non-personal data, the Expert Group has decided to content itself with a statement which merely signals the issues and recommends that Member countries should work towards their solution.

Follow-up

77. The Expert Group called attention to the terms of Recommendation 4 on the Guidelines which suggests that Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of the Guidelines.

DECLARATION ON TRANSBORDER DATA FLOWS

DECLARATION ON TRANSBORDER DATA FLOWS

(Adopted by the Governments of OECD Member countries on 11th April 1985)

Rapid technological developments in the field of information, computers and communications are leading to significant structural changes in the economies of Member countries. Flows of computerised data and information are an important consequence of technological advances and are playing an increasing role in national economies. With the growing economic interdependence of Member countries, these flows acquire an international dimension, known as Transborder Data Flows. It is therefore appropriate for the OECD to pay attention to policy issues connected with these transborder data flows.

This declaration is intended to make clear the general spirit in which Member countries will address these issues.

In view of the above, the GOVERNMENTS OF OECD MEMBER COUNTRIES:

> Acknowledging that computerised data and information now circulate, by and large, freely on an international scale;
>
> Considering the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the significant progress that has been achieved in the area of privacy protection at national and international levels;
>
> Recognising the diversity of participants in transborder data flows, such as commercial and non-commercial organisations, individuals and governments, and recognising the wide variety of computerised data and information, traded or exchanged across national borders, such as data and information related to trading activities, intracorporate flows, computerised information services and scientific and technological exchanges;

Recognising the growing importance of transborder data flows and the benefits that can be derived from transborder data flows; and recognising that the ability of Member countries to reap such benefits may vary;

Recognising that investment and trade in this field cannot but benefit from transparency and stability of policies, regulations and practices;

Recognising that national policies which affect transborder data flows reflect a range of social and economic goals, and that governments may adopt different means to achieve their policy goals;

Aware of the social and economic benefits resulting from access to a variety of sources of information and of efficient and effective information services;

Recognising that Member countries have a common interest in facilitating transborder data flows, and in reconciling different policy objectives in this field;

Having due regard to their national laws, do hereby DECLARE THEIR INTENTION TO:

1. *Promote* access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;

2. *Seek* transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;

3. *Develop* common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;

4. *Consider* possible implications for other countries when dealing with issues related to transborder data flows.

Bearing in mind the intention expressed above, and taking into account the work being carried out in other international fora, the GOVERNMENTS OF OECD MEMBER COUNTRIES:

> *Agree* that further work should be undertaken and that such work should concentrate at the outset on issues emerging from the following types of transborder data flows:
>
> 1. Flows of data accompanying international trade;
>
> 2. Marketed computer services and computerised information services; and
>
> 3. Intracorporate data flows.

The GOVERNMENTS OF OECD MEMBER COUNTRIES AGREED to *co-operate* and *consult* with each other in carrying out this important work, and in furthering the objectives of this Declaration.

GUIDELINES ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS

DECLARATION ON THE PROTECTION OF PRIVACY ON GLOBAL NETWORKS

(made by OECD Ministers at the Conference
"A Borderless World: Realising the Potential of Global Electronic Commerce"
7-9 October 1998, Ottawa, Canada)

The Governments of OECD Member Countries*:

Considering that the development and diffusion of digital computer and network technologies on a global scale offer social and economic benefits by encouraging information exchange, increasing consumer choice, and fostering market expansion and product innovation;

Considering that global network technologies facilitate the expansion of electronic commerce, and accelerate the growth of transborder electronic communications and transactions among governments, businesses, and users and consumers;

Considering that personal data should be collected and handled with due respect for privacy;

Considering that digital computer and network technologies enhance traditional methods for processing personal data, increase the ability to collect, gather and link large quantities of data, and to produce augmented information and consumer profiles;

Considering that digital computer and network technologies can also be used to educate users and consumers about online privacy issues and to assist them to maintain their anonymity in appropriate circumstances or to exercise choice with respect to the uses made of personal data;

---

* including the European Communities.

Considering that in order to increase confidence in global networks, users and consumers need assurances about the fair collection and handling of their personal data, including data about their online activities and transactions;

Considering that it is necessary to ensure the effective and widespread protection of privacy by businesses which collect or handle personal data in order to increase user and consumer confidence in global networks;

Considering that transparent rules and regulations governing the protection of privacy and personal data and their effective implementation on information networks are key elements to increasing confidence in global networks;

Considering that different effective approaches to privacy protection developed by Member countries, including the adoption and implementation of laws or industry self-regulation, can work together to achieve effective privacy protection on global networks;

Considering the need for global co-operation and the necessity of industry and business taking a key role, in co-operation with consumers and governments, to provide effective implementation of privacy principles on global networks;

Considering that the technology-neutral principles of the 1980 OECD Privacy Guidelines continue to represent international consensus and guidance concerning the collection and handling of personal data in any medium, and provide a foundation for privacy protection on global networks;

REAFFIRM the objectives set forth in:

The Recommendation Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, adopted by the Council of the OECD on 23rd September 1980 (OECD Privacy Guidelines);

The Declaration on Transborder Data Flows, adopted by the Governments of OECD Member countries on 11th April 1985; and

The Recommendation concerning Guidelines for Cryptography Policy, adopted by the Council of the OECD on 27th March 1997.

DECLARE THAT:

They will reaffirm their commitment to the protection of privacy on global networks in order to ensure the respect of important rights, build confidence in global networks, and to prevent unnecessary restrictions on transborder flows of personal data;

They will work to build bridges between the different approaches adopted by Member countries to ensure privacy protection on global networks based on the OECD Guidelines;

They will take the necessary steps, within the framework of their respective laws and practices, to ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks, and in particular:

encourage the adoption of privacy policies, whether implemented by legal, self-regulatory, administrative or technological means;

encourage the online notification of privacy policies to users;

ensure that effective enforcement mechanisms are available both to address non-compliance with privacy principles and policies and to ensure access to redress;

promote user education and awareness about online privacy issues and the means at their disposal for protecting privacy on global networks;

encourage the use of privacy-enhancing technologies; and

encourage the use of contractual solutions and the development of model contractual solutions for online transborder data flows;

They agree to review progress made in furtherance of the objectives of this Declaration within a period of two years, and to assess the need for further action to ensure the protection of personal data on global networks in pursuit of these objectives.

FURTHER DECLARE THAT THE OECD SHOULD:

Support Member countries in exchanging information about effective methods to protect privacy on global networks, and to report on their efforts and experience in achieving the objectives of this Declaration;

Examine specific issues raised by the implementation of the OECD Privacy Guidelines in relation to global networks and, after collection and distribution of examples of experiences on implementation of the Guidelines, provide practical guidance to Member countries on the implementation of the Guidelines in online environments, taking into account the different approaches to privacy protection adopted by Member countries and drawing on the experiences of Member countries and the private sector;

Co-operate with industry and business as they work to provide privacy protection on global networks, as well as with relevant regional and international organisations;

Periodically review the main developments and issues in the field of privacy protection with respect to the objectives of this Declaration;

Take into account, *inter alia*, in its future work, the issues and suggested activities discussed in the Background Report accompanying this Declaration.

INVITE:

Non-member countries to take account of this Declaration;

Relevant international organisations to take this Declaration into consideration as they develop or revise international conventions, guidelines, codes of practice, model contractual clauses, technologies and interoperable platforms for protection of privacy on global networks;

Industry and business to take account of the objectives of this Declaration and to work with governments to further them by implementing programmes for the protection of privacy on global networks.

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(93 2002 01 1 P) ISBN 92-64-19719-2 – No. 52355 2002