Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

(ETS No. 108)

Français

Explanatory Report

I. The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, drawn up within the Council of Europe by a committee of governmental experts under the authority of the European Committee on Legal Co-operation (CDCJ), was opened for signature by the member States of the Council of Europe on 28 January 1981 in Strasbourg, on the occasion of the third part of the 32nd Session of the Consultative Assembly.

II. The text of the explanatory report prepared by the committee of experts and submitted to the Committee of Ministers of the Council of Europe, as amended by the CDCJ does not constitute an instrument providing an authoritative interpretation of the text of the Convention, although it might be of such nature as to facilitate the understanding of the provisions contained therein.

Introduction

Data protection

1. The object of this convention is to strengthen data protection, i.e. the legal protection of individuals with regard to automatic processing of personal information relating to them.

There is a need for such legal rules in view of the increasing use made of computers for administrative purposes. Compared with manual files, automated files have a vastly superior storage capability and offer possibilities for a much wider variety of transactions, which they can perform at high speed.

Further growth of automatic data processing in the administrative field is expected in the coming years *inter alia* as a result of the lowering of data processing costs, the availability of "intelligent" data processing devices and the establishment of new telecommunication facilities for data transmission.

2. "Information power" brings with it a corresponding social responsibility of the data users in the private and public sector. In modern society, many decisions affecting individuals are based on information stored in computerised data files: payroll, social security records, medical files, etc. It is essential that those responsible for these files should make sure that the

undeniable advantages they can obtain from automatic data processing do not at the same time lead to a weakening of the position of the persons on whom data are stored. For this reason, they should maintain the good quality of the information in their care, refrain from storing information which is not necessary for the given purpose, guard against unauthorised disclosure or misuse of the information, and protect the data, hardware and software against physical hazards.

3. The established legal systems of the member States are not entirely devoid of rules which can help to accomplish these aims. They have laws on privacy, tort, secrecy or confidentiality of sensitive information, etc.

However, there is a lack of general rules on the storage and use of personal information and in particular, on the question of how individuals can be enabled to exercise control over information relating to themselves which is collected and used by others.

Action of the Council of Europe

4. In 1968, the Parliamentary Assembly of the Council of Europe addressed Recommendation 509 to the Committee of Ministers asking it to examine whether the European Human Rights Convention and the domestic law of the member States offered adequate protection to the right of personal privacy vis-à-vis modern science and technology.

A study carried out on instruction of the Committee of Ministers in response to that recommendation showed that the present national legislations gave insufficient protection to individual privacy and other rights and interests of individuals with regard to automated data banks.

On the basis of these findings, the Committee of Ministers adopted in 1973 and 1974 two resolutions on data protection. The first, Resolution (73) 22 established principles of data protection for the private sector and the second, Resolution (74) 29 did the same for the public sector.

National legislation

5. The resolutions listed a number of ground rules to be observed when personal information is stored in electronic data banks. Although it was left to the discretion of the member States by what means they would give effect to these rules, it should be noted that practically all those States have decided or are considering to do so by legislation.

Within five years after the passing of the second resolution, general data protection laws have been enacted in seven member States (Austria, Denmark, France, Federal Republic of Germany, Luxembourg, Norway and Sweden). In three member States, data protection has been incorporated as a fundamental right in the Constitution (Article 35 of the 1976 Constitution of Portugal; Article 18 of the 1978 Constitution of Spain; Article 1 of the 1978 Austrian Data Protection Act: Fundamental Right of Data Protection).

The Parliamentary Assembly of the Council of Europe, taking the latter tendency into account, has recommended the Committee of Ministers in its Recommendation 890 (1980) to study the possibility of including in the Human Rights Convention a provision on the protection of personal data.

In many other member States (notably Belgium, Iceland, the Netherlands, Spain and Switzerland) legislation on data protection is in an advanced state of preparation.

6. The general characteristics of this legislation are in conformity with the principles set out in the Committee of Ministers' Resolutions (73) 22 and (74) 29. All national data protection laws, as well as the proposals for legislation which have been made public, contain similar rules on the substantive law relating to processing of personal data, i.e. on the quality of the data and on the way in which they may be used.

While the procedural rules differ from one country to another, in keeping with its general system, there is a large measure of agreement on the objectives to be satisfied by these rules. All national laws recognise: i. the principle of publicity, i.e. that the existence of automated data files should be publicly known; and ii. the principle of control, i.e. that public supervisory authorities as well as the individuals directly concerned by the information can require that the rights and interests of those individuals are respected by the data users.

7. In most countries the data protection law has, or will have, a wide scope and apply to data processing in the public sector as well as the private sector. In some countries, moreover, not only automated files but also certain categories of manual files fall within its area of application. In all countries the legislation covers data relating to natural persons, but in some it also covers data concerning legal persons. Where, for reasons of public interest, certain restrictions or exceptions from the general rules are necessary, these are generally spelled out by the law itself.

Transborder flows of personal data

8. The question has arisen to what extent national data protection laws afford adequate protection to individuals when data concerning them flow across borders. Computers, in combination with telecommunications, are opening new prospects for data processing on an international scale. They help to overcome several types of barrier to communication between nations: distance, time, language and cost. Distributed processing enables users to disperse an information system or data base over several countries. Networks help users to have access to or link information systems in distant countries. In several sectors (for example banking, travel, credit cards, etc.) such transfrontier data processing applications are already commonplace.

9. In principle, it should make no difference for data users or data subjects whether data processing operations take place in one or in several countries. The same fundamental rules should apply and data subjects should be given the same safeguards for the protection of their rights and interests.

In practice, however, protection of persons grows weaker when the geographic area is widened. Concern has been expressed that data users might seek to avoid data protection controls by moving their operations, in whole or in part, to "data havens", i.e. countries which have less strict data protection laws, or none at all.

In order to counter this risk some countries have built into their domestic law special controls, for example in the form of a licence for export.

However, such controls may interfere with the free international flow of information which is a principle of fundamental importance for individuals as well as nations. A formula had to be found to make sure that data protection at the international level does not prejudice this principle.

The need for an international agreement

10. Even between States which have a very similar system of data protection law, problems arise both with regard to the law itself and its practical application. When automatic processing of personal data involves parties in different countries (for example, a data bank in one country linked to terminals in other countries) it may not always be easy to determine which State has jurisdiction and which national law applies.

Furthermore, persons resident in one country may encounter difficulties when they want to exercise their rights with regard to automated data files in other countries. Such problems can only be satisfactorily solved through international co-operation.

11. More generally, having regard to the rapid evolution of information handling techniques and the development of international data traffic, it is desirable to create mechanisms at the international level which enable States to keep each other informed and to consult each other on matters of data protection.

Terms of reference for the convention

12. In 1972, when a committee of experts was preparing the resolutions on data protection (see paragraph 5), it emphasised that the next step after enactment of national legislation based on these resolutions should be the reinforcement of these national rules by means of a binding international agreement. A similar suggestion was made by the 7th Conference of European Ministers of Justice (Basle, 1972) in its Resolution No. 3.

The committee considered two models for such an agreement. The first was based on reciprocity: one country would not allow in its territory data processing operations relating to persons resident in another country if such operations would be illegal under the laws of that country.

This model was based on the assumption that each country would apply its own data protection standards. Apart from the practical implications which it entailed, the model was contrary to the idea that all persons should enjoy basically the same rights. The committee therefore expressed its preference for a second model based on data protection principles common to all Parties.

13. In 1976, the Committee of Ministers instructed the Committee of Experts on Data Processing, placed under the aegis of the European Committee for Legal Co-operation (CDCJ) "...to prepare a convention for the protection of privacy in relation to data processing abroad and transfrontier data processing" (Activity No. 21.20.1 of the Programme of Intergovernmental Activities).

Co-operation with OECD and the EEC

14. The committee was instructed to do so in close collaboration with the Organisation for Economic Co-operation and Development, as well as the non-European member countries of that organisation, having regard to the activities which OECD was carrying out in the field of information, computer and communications policy. Close liaison was maintained between the two organisations both at the Secretariat level and at the level of the Council of Europe's committee of experts and the corresponding OECD committee, the Data Bank Panel, which was succeeded in 1978 by an expert group on transborder data barriers. The latter group was instructed by the OECD Council to develop privacy protection guidelines, to facilitate harmonisation of national legislations of the OECD member countries, without this precluding at a later date the establishment of an international convention.

15. OECD, as well as four of its non-European member countries (Australia, Canada, Japan and the United States) were represented by an observer on the Council of Europe's committee. Observers from Finland, the Hague Conference on Private International Law and the European Communities also took part in the work.

16. The Commission of the European Communities, which carried out studies concerning harmonisation of national legislation within the Community in relation to transborder data flows and possible distortions of competition, as well as problems of data security, kept in close touch with the Council of Europe. The Commission decided to await the outcome of the work on this convention before deciding on its own action in the field of data protection. The European Parliament also expressed a deep interest in data protection. At its May 1979 session it adopted a resolution on the protection of the rights of the individual in the face of technical developments in data processing which it forwarded to the Committee of Ministers of the Council of Europe.

The work of the Committee of Experts on Data Protection

17. From November 1976 to May 1979, the Committee of Experts on Data Protection held four meetings, first under the chairmanship of Mr L. Joinet (France), and subsequently under that of Mr R. A. Harrington (United Kingdom). A working party composed of the experts from Austria, Belgium, France, Federal Republic of Germany, Italy, Netherlands, Spain, Sweden, Switzerland and the United Kingdom, met several times between the plenary committee meetings, to work out the general philosophy as well as the details for the draft convention.

In April 1980 another committee of experts, chaired by Mr J. Voyame (Switzerland), revised and finalised the text. This was approved by the CDCJ at its 33rd meeting and adopted by the Committee of Ministers, which decided to open it for signature on 28 January 1981.

Chief characteristics of the convention

18. The convention consists of three main parts:

- substantive law provisions in the form of basic principles;
- special rules on transborder data flows;

– mechanisms for mutual assistance and consultation between the Parties.

19. The convention's point of departure is that certain rights of the individual may have to be protected vis-à-vis the free flow of information regardless of frontiers, the latter principle being enshrined in international and European instruments on human rights (see Article 10, European Human Rights Convention; Article 19, International Covenant on Civil and Political Rights). Where the present convention imposes certain restrictions or conditions on the exercise of freedom of information, it does so only to the extent strictly justified for the protection of other individual rights and freedoms, in particular the right to respect for individual privacy (see Article 8, European Human Rights Convention).

It does not seem advisable, however, to rely solely on the European Human Rights Convention for data protection, *inter alia* because it is a "closed" instrument, which does not permit the participation of non-European and non-member States.

20. The central part of the convention is Chapter II, in which are laid down basic principles for data protection. Each Party should take the necessary steps to give effect to this "common core" in its domestic legislation. The point of departure for these provisions is the principles laid down earlier in the Committee of Ministers' Resolutions (73) 22 and (74) 29, these principles being completed, where appropriate, in the light of subsequent legislative developments in the member States.

It should be noted that the convention gives clear and precise indications on the purpose to be achieved by each principle, but leaves to each Party, the manner of implementing it in its domestic law.

The "common core" principles guarantee to data subjects in all countries where the convention is in force a certain minimum protection with regard to automatic data processing of personal data. By undertaking to apply these principles the Parties tend mutually to renounce restrictions to transborder data flows and thus they avoid that the principle of free flow of information would be jeopardised by any form of protectionism. Moreover, the "common core" will result in a harmonisation of the laws of the Contracting States and hence decrease the possibility of conflicts of law or jurisdiction.

21. Chapter III (concerning transborder data flows) aims at reconciling the simultaneous and sometimes competing requirements of free flow of information and data protection, the main rule being that transborder data flows between Contracting States should not be subject to any special controls. This provision should be seen in close conjunction with Chapter II which ensures that the processing of personal data is subject in all countries concerned to the same fundamental rules ("common core").

22. Chapters IV and V provide mechanisms for co-operation between the Contracting States, both in individual cases (Chapter IV, mutual co-operation between authorities and assistance to data subjects abroad) and with regard to the convention as a whole (Chapter V).

The formula used here permits restricting the contents of the convention to the basic principles and relying on co-operation between States, in the

framework of a consultative committee, for the implementation and harmonisation of these principles in their domestic law.

23. The committee of experts has also given attention to the question whether the convention should lay down rules with regard to problems of applicable law. These problems may arise when data processing operations are carried out on the territory of two or more States (contracting or non-contracting) or when parties concerned by data processing, particularly the data subjects and the data users, reside in different countries. The committee decided that it was premature to include in the convention specific rules on this subject. The presence of a "common core" of substantive law (Chapter II), parts of which harmonise procedure, will help to reduce the risk of conflict of laws or legal lacunae. The committee agreed, however, that the problem of applicable law should be kept under review and that at a later stage provisions relating to it should, if necessary, be laid down in a protocol to the convention.

Commentary on the provisions of the Convention

Title

24. The title describes this instrument as "Convention", not as "European Convention" in order better to underline that there ought to be ample scope for accession to it by non-European States.

Preamble

25. The preamble reaffirms the commitment of the signatory States to human rights and fundamental freedoms. Moreover, it acknowledges that the unfettered exercise of the freedom to process information may, under certain conditions, adversely affect the enjoyment of other fundamental rights (for example privacy, non-discrimination, fair trial) or other legitimate personal interests (for example employment, consumer credit). It is in order to maintain a just balance between the different rights and interests of individuals that the convention sets out certain conditions or restrictions with regard to the processing of information. No other motives could justify the rules which the Contracting States undertake to apply in this field.

It is also underlined that the convention should not be interpreted as a means to erect non-tariff barriers to international trade or to restrain the exchange of scientific and cultural information.

Chapter 1 – General provisions

Article 1 – Object and purpose

26. The first article is devoted to a description of the convention's object and purpose.

The guarantees set out in the convention are extended to every individual regardless of nationality or residence. This provision is in accordance with the general principle of the Council of Europe and its member States with regard to the protection of individual rights. Clauses restricting data protection to a State’s own nationals or legally resident aliens would be incompatible with the convention.

Article 2 – Definitions

27. Definitions used in this convention are meant to cover, where necessary, different terms or concepts used in national legislation to express certain fundamental concepts. The terms and definitions generally follow those used in Resolutions (73) 22 and (74) 29. Some modifications and additions have been made in view of recent national legislation and having regard to the special problems called forth by transfrontier data flows.

Litt. a

28. "Identifiable persons" means a person who can be easily identified: it does not cover identification of persons by means of very sophisticated methods.

29. The notion of "data subject" expresses the idea that a person has a subjective right with regard to information about himself, even where this is gathered by others.

Litt. b

30. The definition covers not only data files consisting of compact sets of data, but also sets of data which are geographically distributed and are brought together via computer links for purposes of processing.

The term "automated data file" has replaced the term "electronic data bank", previously used in Resolutions (73) 22 and (74) 29 and in some national laws. "Data bank" is used today in a more specialised sense: a pool of data accessible to several users.

Litt. c

31. Subject to the provisions of Articles 5.a and 12, the collection of information falls outside the notion of "processing".

In view of the rapid development of data processing technology it was found advisable to formulate a fairly general definition of "automatic data processing", capable of flexible interpretation.

"Dissemination" is a broad term which covers both disclosure of information to a person (or several persons) and enabling persons to consult the information.

Litt. d

32. By "controller of the file" the convention means only the person or body ultimately responsible for the file, not persons who carry out the operations according to the instructions given by the controller of the file.

The reference to the "national law" takes into account the fact that the various national data protection laws contain precise criteria for determining who is the competent person.

Under the terms of Article 8.a, it should always be possible to discover the identity of the controller of the file.

Article 3 – Scope

33. According to *paragraph 1* the convention applies to the public as well as the private sector. Although most international data traffic occurs in the private sector, the convention is nevertheless of great importance for the public sector and this for two reasons. First, Article 3 imposes obligations on the member States to apply data protection principles even when they process public files – as is usually the case – entirely within their national borders. Secondly, the convention offers assistance to data subjects who wish to exercise their right to be informed about their record kept by a public authority in a foreign country.

The distinction public sector/private sector is not found in the other provisions of the convention, especially since these terms may have a different meaning in different countries. But it may play a role in the declarations which the Parties may make with regard to the scope of the convention (paragraph 2).

34. *Paragraph 2.a.* It should be emphasised that exclusions from the scope of the convention are permitted only with respect to those categories of data files which are not or not yet subject to data protection legislation domestically.

As for categories of data files which are subject to such legislation, derogations are permitted only under Article 9.

35. It is understood that any exceptions must be clearly specified. Otherwise, problems of interpretation would arise for other Contracting States to determine the scope of an exception, thus seriously hampering the application of the convention.

36. *Paragraphs 2.b and* c. These paragraphs enable States to extend the protection offered under the convention to data subjects who are not physical persons and to manual data files. These States may invoke the rule of reciprocity with regard to States who have not made such extensions (paragraph 4).

37. *Paragraph 5* determines the moment at which the declarations referred to in this article will take effect and also the procedure to be followed for their withdrawal.

Chapter II – Basic principles of data protection

Article 4 – Duties of the Parties

38. As this article indicates, the convention obliges Parties to incorporate data protection provisions into their domestic legislation. The convention was not designed to be self-executing, with the result that individual rights cannot be derived from it.

39. The "measures within its domestic law" can take different forms, depending on the legal and constitutional system of the State concerned: apart from laws they may be regulations, administrative guidelines, etc.

Such binding measures may usefully be reinforced by measures of voluntary regulation in the field of data processing, such as codes of good practice or codes for professional conduct. However, such voluntary measures are not by themselves sufficient to ensure full compliance with the convention.

It is further stipulated that the measures giving effect to the convention should be in force at the time when the convention takes effect with regard to the country concerned in order to avoid a legal vacuum between the date of entry into force of the convention and the date on which the domestic measures will take effect. If ' for valid reasons, the domestic law does not yet apply to certain kinds of records, an exclusion should be made under Article 3.a,

Article 5 – Quality of data

40. The provisions of this article are largely identical to the corresponding principles laid down in Resolutions (73) 22 and (74) 29 and can also be found in very similar terms in the national data protection laws enacted prior to this convention.

The different provisions of this article aim at the fulfilment of two fundamental legal standards. On the one hand the information should be correct, relevant and not excessive in relation to its purpose. On the other hand its use (gathering, storage, dissemination) should likewise be correct.

41. The reference to "purposes" in litterae b and c indicates that it should not be allowed to store data for undefined purposes. The way in which the legitimate purpose is specified may vary in accordance with national legislation.

42. The requirement appearing under littera e concerning the time-limits for the storage of data in their name-linked form does not mean that data should after some time be irrevocably separated from the name of the person to whom they relate, but only that it should not be possible to link readily the data and the identifiers.

Article 6 – Special categories of data

43. While the risk that data processing is harmful to persons generally depends not on the contents of the data but on the context in which they are used, there are exceptional cases where the processing of certain categories of data is as such likely to lead to encroachments on individual rights and interests. Categories of data which in all member States are considered to be especially sensitive are listed in this article.

44. The expression "revealing ... political opinions, religious or other beliefs" covers also activities resulting from such opinions or beliefs.

45. The meaning of the term "personal data concerning health" has been carefully studied by the Committee of Experts on Data Protection in connection with its work on medical data banks. It includes information concerning the past, present and future, physical or mental health of an individual. The information may refer to a person who is sick, healthy or deceased. This category of data also covers those relating to abuse of alcohol or the taking of drugs.

46. In the same way as under Article 4 (paragraph 39 above) the expression "domestic law" may be taken in a wide sense, i.e. not only legislation but also appropriate or specific regulations or administrative directives, as long as the necessary level of protection is secured.

47. By "criminal convictions" in the sense of this article should be understood: convictions based on criminal law and in the framework of a criminal procedure.

48. The list of this article is not meant to be exhaustive. A Contracting State may, in conformity with Article 11, include in its domestic law other categories of sensitive data, the processing of which is prescribed or restricted. The degree of sensitivity of categories of data depends on the legal and sociological context of the country concerned. Information on trade union membership for example may be considered to entail as such a privacy risk in one country, whereas in other countries it is considered sensitive only in so far as it is closely connected with political or religious views.

Article 7 – Data security

49. There should be specific security measures for every file, taking into account its degree of vulnerability, the need to restrict access to the information within the organisation, requirements concerning long-term storage, and so forth. The security measures must be appropriate, i.e. adapted to the specific function of the file and the risks involved They should be based on the current state of the art of data security methods and techniques in the field of data processing.

Article 8 – Additional safeguards for the data subject

50. The provisions set out in this article are designed to enable a data subject to defend his rights vis-à-vis automated data files. Although in domestic legislation the contents of Article 8 clearly correspond to subjective rights, the present text expresses them in the form of safeguards which Contracting States offer to data subjects, in view of the non self-executing character of the convention. These safeguards include four main elements:

– knowledge about the existence of an automated data file;

– knowledge about the contents of the information, if any, stored about data subjects in a file;

– rectification of erroneous or inappropriate information;

– a remedy if any of the previous elements are not respected.

51. In order that these rights can be effective, the convention requires that with regard to every automated record it should be stated clearly who is the controller (littera a). The wording of this littera takes into account the variety of rules of domestic law giving effect to this principle. There are States where the name of the controller of the file is listed in a public index. In other States which have no such publicity rule, the law will provide that the name of the controller of the file must be communicated to a person at his request.

52 ln litterae b and c it has not been specified from whom a data subject may obtain confirmation, communication, rectification, etc. In most States this will be the controller of the file, but in some States this right is exercised through the intermediary of the supervisory authority.

53. The wording of littera b is intended to cover various formulas followed by national legislation: communication at the request of the data subject or at the initiative of the controller of the file; communication free of charge at fixed intervals as well as communication against payment at any other time, etc. The term "expense" means the fee charged to the data subject, not the actual cost of the operation.

54. In the case of rectifications obtained in conformity with the principle set out in littera c, national law or practice provides usually that where appropriate those rectifications should be brought to the recipients of the original information.

Article 9 – Exceptions and restrictions

55. Exceptions to the basic principles for data protection are limited to those which are necessary for the protection of fundamental values in a democratic society. The text of the second paragraph of this article has been modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human Rights Convention. It is clear from the decisions of the Commission and the Court of Human Rights relating to the concept of "necessary measures" that the criteria for this concept cannot be laid down for all countries and all times, but should be considered in the light of the given situation in each country.

56. Littera a *in paragraph 2* lists the major interests of the State which may require exceptions. These exceptions are very specific in order to avoid that, with regard to the general application of the convention, States would have an unduly wide leeway.

States retain, under Article 16, the possibility to refuse application of the convention in individual cases for important reasons, which include those enumerated in Article 9.

The notion of "State security" should be understood in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State.

57. The term "monetary interests of the State" covers all the different means of financing a State's policies. Accordingly, the term refers in particular to tax collection requirements and exchange control. The term "suppression of criminal offences" in this littera includes the investigation as well as the prosecution of criminal offences.

58. Littera b concerns major interests of private parties, such as those of the data subject himself (for example psychiatric information) or of third parties (for example freedom of the press, trade secrets, etc.).

59. Paragraph 3 leaves the possibility of restricting the exercise of the data subjects' rights with regard to data processing operations which pose no risk. Examples are the use of data for statistical work, in so far as these data are presented in aggregate form and stripped of their identifiers.

Similarly, and in conformity with a recommendation of the European Science Foundation, scientific research is included in this category.

Article 10 – Sanctions and remedies

60. In order that this convention can guarantee effective data protection, the duties of the data users and the rights of data subjects should be reflected in the national legislation of member States by corresponding sanctions and remedies.

In keeping with the non self-executing character of the convention, it should be left to each State to determine the nature of these sanctions and remedies (civil, administrative, criminal).

Article 11 – Extended protection

61. This article has been based on a similar provision, Article 60, of the European Human Rights Convention. The convention confirms the principles of data protection law which all Contracting States are ready to adopt. It is underlined in the text that these principles constitute only a basis on which States may build a more advanced system of protection.

Chapter III – Transborder data flows

Article 12

62. The aim of this article is to reconcile the requirements of effective data protection with the principle of free flow of information, regardless of frontiers, which is enshrined in Article 10 of the European Human Rights Convention.

63. *Paragraph* 1, specifying the scope of transborder data flows, has been so worded as to take into account the wide variety of factors determining the way in which data are transferred: mode of representation of the data (plain text, encoded text); their storage medium (paper, punched card, punched tape, magnetic tape, disk, etc.); way of transport (physical transport, mail, circuit-switched or packet-switched telecommunications link); interface (computer to terminal, computer to computer, manual to computer, etc.); the circuit followed (direct from country of origin to country of destination, or via one or more countries of transit); the relations between the sender and recipient (within one organisation or different organisations) etc.

64. According to paragraph 1, the provisions of Article 12 also apply to data collection. This extension was considered indispensable in order to avoid that data gathered in one country and processed in another would escape the rules set out in this convention.

65. This paragraph sets out clearly that the provisions of Article 12 apply only to transborder data flows of personal data. It is understood, however, that if two or more Contracting States have declared the convention applicable to information on legal persons (according to the option they have under Article 3, paragraph 2.b), Article 12, and indeed all other articles of the convention, apply to such information, but only between the States who have exercised this option. On the other hand a Contracting State, which has excluded from the scope of the convention, on the basis of

Article 3, paragraph 2.a, certain categories of data shall be, in fact, so far as those data are concerned in the same position as a non-Contracting State.

66. So far as the data transfers mentioned in paragraph 1 are concerned, Article 12 actually will affect only the export of data, not their import. The latter presents no problems because imported data are in any case covered by the data protection regime of the importing State. Some problems might, however, arise in case of re-import of data processed abroad in violation of certain provisions of the law of the country of origin Party to the convention. But it is clear in such cases that it is up to the country of origin to take, before export, the necessary measures according to Article 12.

67. Paragraphs 2 and 3 deal with the measures which States may apply in order to ensure that transborder data flows should not result in eroding the protection of persons, at home or abroad, vis-à-vis data processing carried out partly or wholly in their territory.

The main rule (paragraph 2) is that in principle there shall not be permitted between Contracting States obstacles to transborder data follows in the form of prohibitions or special authorisations of data transfers. The rationale for this provision is that all Contracting States, having subscribed to the common core of data protection provisions set out in Chapter II, offer a certain minimum level of protection.

This rule does not mean that a Contracting State may not take certain measures to keep itself informed of data traffic between its territory and that of another Contracting State, for example by means of declarations to be submitted by controllers of data files.

The expression "for the sole purpose of the protection of privacy" adds an important clarification, namely that a Contracting State may not invoke this convention to justify interference with transborder data flows for reasons which have nothing to do with the protection of privacy (for example, hidden trade barriers).

Paragraph 2 of this article does not affect the possibility for a Party to lay down in its domestic data protection law provisions which, in particular cases, do not permit certain transfers of personal data irrespective of whether such transfers take place within its territory or across the borders.

68. In some cases transfers will be made from an automated data file in a Party simultaneously to several foreign countries, some of which are Parties to the convention whereas others are non-contracting States. In those cases, the originating Party which has a procedure of export licences may not be able to avoid applying those procedures also to the data destined for a Party, but it should then proceed in such a way as to ensure that a licence for data transfers to the latter Party is agreed.

69. The categories of data or data files mentioned in paragraph 3.a may be those referred to in Article 6, as well as other categories. So far as data mentioned in Article 6 are concerned (for example racial origin, political opinions), a Contracting State may make a derogation under Article 12, paragraph 3.a, if its specific measures protecting those data are substantially different from the legal provisions of other Contracting States on those data, and particularly if those measures offer a level of protection,

in accordance with Article 11, going beyond the minimum rules set out in Chapter II. A further justification for derogation arises where categories of data or data files not specifically mentioned in Article 6 are subject to special safeguards. It is obvious however that a derogation from paragraph 2 is not allowed if the recipient Party provides an equivalent protection. This means, *inter alia,* that a Contracting State which subjects transborder data flows to special authorisation may not deny such authorisation on the ground of protection of privacy if the recipient country provides equivalent protection.

70. Littera b of this paragraph concerns data flows to a non-Contracting State passing through the intermediary of a Contracting State. The wording of this sub-paragraph indicates that the derogation may be invoked only when it is clearly established that the data transferred are actually only passing through the Contracting State. It should not be applied on the mere presumption or expectation that the data transferred to another Contracting State may eventually be passed on to a non-Contracting State. Nor will a State which has a system of authorisations necessarily invoke derogation b for all data traffic to non-Contracting States. It may decide to renounce such authorisations for example because the non-Contracting State in question has a satisfactory data protection regime.

Chapter IV – Mutual assistance

Article 13 – Co-operation between Parties

71. The main provisions of this chapter are based on the two recent European conventions relating to mutual assistance in administrative matters: the European Convention on the Service Abroad of Documents relating to Administrative Matters of 24 November 1977, and the European Convention on the Obtaining Abroad of Information and Evidence in Administrative Matters of 15 March 1978. So far as the Parties to these conventions are concerned, the conclusion of a special agreement in the field of data protection is in conformity with a provision of these conventions according to which the general co-operative framework they have established may be supplemented by separate agreements in specific fields.

72. Among the reasons why in the present case a separate agreement is preferred, there should be mentioned the fact that the present convention is expected to attract a larger number of non-member States than the two conventions mentioned above. Moreover, having regard to the special nature of data protection, many States may in practice wish to entrust mutual assistance in data protection matters to authorities specialised in this field. Most countries having a data protection law also have a special protection authority. It is not unlikely that in many States this authority will be designated as the liaison authority under *paragraph 2.a.*

73. It should be underlined, however, that while the convention requires the designation of an authority by each Contracting State, this does not mean that the convention requires each State to have a data protection authority. A Contracting State may designate an authority for the purposes of the convention only.

74. According to Article 13, the authorities will render each other general assistance for controls *a priori* (for example certifying whether terminals in

one country, linked to a computer centre in another country meet data security requirements) as well as specific assistance for controls *a posteriori* (for example to verify the activities of a specific computer centre). The information may be of a legal or factual character.

75. With regard to the legal information exchanges between States in conformity with *paragraph 3.a,* it has been suggested that such exchanges might be organised not only bilaterally between States concerned but also multilaterally through the Council of Europe's Secretariat. A proposal to that effect has been elaborated separately, in Recommendation No. R (80) 13 on exchange of legal information relating to data protection which was adopted by the Committee of Ministers on 18 September 1980.

76. With regard to factual information, *paragraph 3.b* specifies that States may not reveal to each other the contents of data contained in data files. This provision is an obvious data protection safeguard for the protection of the privacy of the people concerned.

Article 14 – Assistance to data subjects abroad

77. *Paragraph 1* ensures that subjects residing abroad, whether in a Contracting State or in a third country will be enabled to exercise their right to know, and where necessary to rectify, information stored about them in a data file. This is a practical consequence of Article 1, securing protection to "every individual, whatever his nationality or residence...".

78. According to *paragraph 2,* where the data subject resides in another Contracting State he is given the option to pursue his rights either directly in the country where information relating to him is processed, or indirectly, through the intermediary of that country's designated authority.

Moreover, it goes without saying that data subjects residing abroad always have the opportunity to pursue their rights with the assistance of the diplomatic or consular agents of their own country.

Paragraph 3 specifies in order to expedite the procedure and prevent abuse, that requests be as specific as possible.

Article 15 – Safeguards concerning assistance

79. This article ensures that data protection authorities shall be bound by the same obligation to observe discretion and confidentiality toward foreign data protection authorities and persons residing abroad, as they have to observe in their own country.

This provision is of fundamental importance for mutual trust, on which mutual assistance is based.

Article 16 – Refusal of requests for assistance

80. This article states first that Parties are bound to comply with requests for assistance. The grounds for refusal to comply are enumerated exhaustively. They correspond generally with those provided for by other international treaties in the field of mutual assistance.

These grounds are either that the request is incompatible with the powers of the authority or the terms of the convention and particularly with Article 3 regarding the extensions and exclusions every member State may have made to the scope of the convention or that it is at variance with overriding interests of the requested State or the data subject concerned.

81. The term "compliance" which is used in littera c should be understood in the broader sense as covering not only the reply to the request, but also the action preceding it. For example, a requested authority might refuse action not only if transmission to the requesting authority of the information asked for might be harmful for the fundamental rights of the individual, but also if the very fact of seeking the information might prejudice his fundamental rights.

Article 17 – Costs and procedures of assistance

82. The provisions of this article are analogous to those found in other international conventions on mutual assistance.

83. "Experts" in the sense of *paragraph* 1 covers data processing experts whose intervention is required to make test runs or check the data security of an automated data file.

84. With a view to not burdening the convention with a mass of implementing details, *paragraph 3* of this article provides that procedure, forms and language to be used can be agreed between the States concerned. The text of this paragraph does not require any formal procedures but allows also administrative arrangements which may even be confined to specific cases. It is moreover advisable that States leave to the designated authorities the power to conclude such arrangements. The forms of assistance may also vary from case to case. It is obvious that the transmission of a request for access to sensitive medical information will require a different form than routine inquiries about entries in a population record.

Chapter V – Consultative committee

85. The purpose of Articles l8, 19 and 20 is to facilitate the smooth running of the convention and, where necessary, to perfect it.

86. Since the convention contains a new type of law, created to deal with new problems posed by automatic data processing, it can be expected that questions will arise both with regard to the practical application of the convention (Article 19, littera a) and with regard to its meaning (same article, littera d).

A Consultative Committee, composed of representatives of all Parties, will endeavour to formulate proposals or render advice to those Parties for the solution of these problems.

Where necessary, this committee will itself propose amendments to the convention or examine such proposals formulated by a Party or the Committee of Ministers in conformity with Article 21.

87. The nature of the committee and the procedure followed by it are similar to those set up under the terms of other conventions concluded in the framework of the Council of Europe.

It was not held desirable that the committee should take the form of an international data protection authority. Nor was it considered appropriate to entrust to the committee the formal settlement of disputes arising over the application of the convention. Of course, the committee may help to solve difficulties arising between Parties.

Chapter VI – Amendments

Article 21 – Amendments

88. The Committee of Ministers, which adopted the original text of this convention, is also competent to approve any amendments.

In accordance with *paragraph 1* the initiative for amendments may be taken by the Committee of Ministers itself, by the Consultative Committee and by a Party (whether a member State of the Council of Europe or not).

Any proposal for amendment which has not originated with the Consultative Committee should be submitted to it, in accordance with *paragraph 3,* for an opinion.

Chapter VII – Final clauses

Article 22 – Entry into force

89. Since for the effectiveness of the convention a wide geographic scope is considered essential, *paragraph 2* fixes at five the number of ratifications by member States of the Council of Europe necessary for the entry into force.

Article 23 – Accession by non-member States

90. The convention is destined to be an "open" one with a wide geographic scope (see paragraphs 14 and 15). The convention was elaborated in close co-operation with OECD and the non-European member countries of that organisation and it is in particular those countries which one had in mind when this article was drafted.

Article 24 – Territorial clause

91. The application of the convention to remote territories under the jurisdiction of Parties or on whose behalf a Party can make undertakings is of practical importance in view of the use that is made of distant countries for data processing operations either for reasons of cost and manpower or in view of the utilisation of alternating night and daytime data processing capability.

Article 25 – Reservations

92. The rules contained in this convention constitute the most basic and essential elements for effective data protection. For this reason the convention allows no reservations to its provisions, which are, moreover,

reasonably flexible, having regard to the possibility offered by Article 3 (scope) and derogations permitted under certain other articles.

Article 26 – Denunciation

Article 27 – Notification

93. These provisions are in conformity with the customary final clauses contained in European conventions.