UNITED NATIONS

E

Economic and Social Council

Distr.
GENERAL

E/CN.4/1995/75
23 December 1994

ENGLISH
Original: ENGLISH/FRENCH/SPANISH

COMMISSION ON HUMAN RIGHTS
Fifty-first session
Item 14 of the provisional agenda

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Question of the follow-up to the guidelines for the regulation of computerized personal data files

Report of the Secretary-General prepared pursuant to Commission decision 1993/113

CONTENTS

CONTENTS (continued)

Introduction

1. In its decision 1993/113 of 10 March 1993, the Commission on Human Rights, referring to the guidelines for the regulation of computerized personal data files (E/CN.4/1990/72) adopted by the General Assembly in its resolution 45/95 of 14 December 1990, decided to request the Secretary-General to report to the Commission at its fifty-first session:

(a) On the application of the guidelines within the United Nations system;

(b) On information collected from States and intergovernmental, regional and non-governmental organizations concerning the follow-up to the guidelines at the regional and national levels.

2. Pursuant to that decision, the Secretary-General, on 4 May 1994, addressed requests to United Nations organs, bodies and specialized agencies for information on the application of the guidelines within the appropriate sections of the United Nations system.

3. On the same date, requests were also addressed to States and intergovernmental and non-governmental organizations for information concerning the follow-up to the guidelines at the regional and national levels.

4. By 1 December 1994, replies had been received from the following United Nations organs, bodies and specialized agencies: Department for Policy Coordination and Sustainable Development, United Nations Population Fund, United Nations University, International Court of Justice, World Food Programme, International Labour Organisation, Food and Agriculture Organization of the United Nations, World Health Organization, International Maritime Organization, International Atomic Energy Agency.

5. The following Governments have submitted information: Argentina, Central African Republic, Croatia, Germany, Luxembourg, Malta, Norway, Philippines, Saudi Arabia, Spain, Sweden, United Kingdom of Great Britain and Northern Ireland, Yugoslavia.

6. Replies were also received from the following intergovernmental organizations: African Commission on Human and Peoples' Rights, Council of Europe, Interpol.

7. No replies were received from non-governmental organizations.

8. The present report contains a summary of the substantive replies received. Any additional replies will be issued as addenda to this document.

I. APPLICATION OF THE GUIDELINES WITHIN THE UNITED NATIONS SYSTEM

9. From among 62 various United Nations organs, bodies, regional commissions, specialized agencies and related organizations which were addressed, only 10 have replied.

10. The Department for Policy Coordination and Sustainable Development and the United Nations University stated that they had no information to submit concerning the application of the guidelines on computerized personal data files.

11. The International Court of Justice replied that it could not provide any information in this regard since the Court did not yet work with computerized data files.

12. The International Maritime Organization (IMO) stated that IMO subscribed to the principles in the guidelines and would arrange to have them implemented when it moves to the computerization of personal data files for internal purposes.

13. The International Atomic Energy Agency indicated that its Staff Regulations and Staff Rules, as well as the applicable policies and procedures concerning the collection, maintenance and protection of physical and computerized personnel data, conformed to the guidelines as set out in document E/CN.4/1990/72.

14. The United Nations Population Fund also indicated that it abided by all the guarantees provided under the guidelines.

15. The Food and Agriculture Organization of the United Nations and the World Food Programme replied that the computerized personal file system of FAO was mainly used for payroll purposes, i.e. to allow the automatic attribution of payroll-related benefits. It contained only personnel data relating to nationality, sex, date of birth and marital status, and did not include information on race, religion, ethnic group, etc. The files were used for internal purposes only. Personal data were only made available to third parties with the consent of the staff member concerned. A security subsystem had been established to protect the files against unauthorized access and misuse. It was stated that the major principles contained in part A of document E/CN.4/1990/72 were followed by FAO.

16. The International Labour Organisation ILO stated that its Personnel Department had been aware of the United Nations Guidelines for the Regulation of Computerized Personal Data Files for at least two years. When ILO chose to use the United Nations Integrated Management Information System (IMIS) as the basis for its new Personnel and Payroll system (PERSIS), it researched the guidelines and found these detailed in the ILO Conditions of Work Digest, Volume 10, 2/1991.

17. ILO was invited to a meeting sponsored by the Council of Europe in October 1993 on the subject of protection of personal data. The focus was on how international organizations were dealing with this issue. During this meeting all attending organizations shared their current status and problems. This was a second stimulus on the issue.

18. The Personnel Department has reviewed the Guidelines and supports them all. However, guidelines 9 is not applicable to ILO.

19. As the ILO new Personnel System is based on IMIS, it expects that the United Nations Guidelines have already been applied during the construction of the system. From ILO's own review of the kinds of data which ILO will maintain in its version of IMIS (PERSIS), it certainly appears that there is no data being stored which would be considered outside these Guidelines.

20. The ILO problems will be in the area of accuracy - especially with regard to completeness, since it is very costly to continually review data to ensure that new information is entered as it becomes available. ILO intends to develop a "turnaround document". This document would be sent to all staff members and would contain a list of the significant data which are recorded on them. They would be asked to check for accuracy and update, then they would return this to the Personnel Department for processing. This helps satisfy both guidelines 2 and 4.

21. With regard to manual data files, ILO also agreed that the Guidelines are acceptable. Formerly, ILO had a system of two manual personnel files (A and B). The staff member was not allowed to access his/her B file. This is in the process of being changed. No new B files are created, and the old ones are being processed and will soon be available for access by the staff member concerned.

22. Currently ILO does not have a specific person designated as the authority responsible for supervising these guidelines. While ILO had produced some Conventions and Recommendations on the subject of personal data, it has not yet adopted its own set of guidelines to govern the management of personal data within ILO.

23. It was added that the ILO Conditions of Work and Welfare Facilities Branch had produced two further volumes of the "Conditions of Work Digest", which also touched on aspects of the treatment of computerized data files.

24. The World Health Organization (WHO) submitted the following information:

Budget and finance

25. All personal files in this area are basically confidential. WHO's Administration and Finance Information System (AFI) is operated on a "need-to-know" basis.

Information system management

26. The responsible Division within WHO is the Division of Information System Management (ISM). ISM undertakes some development of computer applications. However, ISM develops common or corporate information systems, which are those systems that are for the use of all WHO programmes/divisions, in contrast to unique systems used by only one organizational element. In this regard, there are no common information systems that contain personal data files other than data that are in the Personnel component of the AFI System supported by the Division of Budget and Finance and our interpretation of the referenced Guidelines is that these data are not considered personal data per se.

27. ISM assists programmes/divisions in finding consultants to develop the unique systems that they may require. To our knowledge, programmes/divisions do not have unique systems containing personal data other than the above-mentioned Personnel component.

Personnel

28. The personal files kept by the Division of Personnel are operated in conformity with the guidelines referred to in United Nations document E/CN.4/1990/72.

II. INFORMATION RECEIVED FROM STATES

A. Argentina

[Original: Spanish]
[12 October 1994]

29. The Constituent National Convention, which on 25 May 1994 began its work on the reform of the National Constitution, on 22 August adopted a text which entered into force on 24 August. In accordance with the amendments made to the text of the Constitution, a new chapter entitled "New Rights and Guarantees" has been incorporated in Part I of the Constitution. In this context article 43 establishes at the constitutional level the remedy of amparo, which already exists in ordinary legislation. The third paragraph of article 43 reads:

> "Any person may apply for this remedy in order to have access to the data relating to him and to learn the purpose of such data in public registers or data banks or private registers or data banks intended to provide information, and in the event of inaccuracy or discrimination, to demand the deletion, rectification, confidentiality or updating of these data. The secrecy of information sources for purposes of journalism may not be affected".

Habeas data is thus expressly authorized by means of a constitutional provision.

B. Central African Republic

[Original: French]
[13 July 1994]

30. The Government of the Central African Republic is determined to do everything possible to ensure observance of the guidelines in question by incorporating them within its national legislation and regulations on this question. All authorities in the Central African Republic have accordingly received a copy of document E/CN.4/1990/72 relating to these guidelines in order that they may duly take them into account.

C. Croatia

[Original: English]
[1 September 1994]

31. In the Republic of Croatia, personal data concerning civil status (registers of births, marriages and deaths, registers of citizenship, and voting rolls) are recorded by computer in most places; however, in some places these records are still kept by hand only.

32. It is under the jurisdiction of the Ministry of Administration to supervise the government administrative bodies which keep State registers of voting rolls and registers of birth, marriages and deaths. Voting rolls are State registers of citizens with voting rights. Registers of births, marriages, and deaths comprise data stipulated by law for each of these facts.

33. Records of citizenship (registers of citizenship) are kept by government administrative bodies - general administration offices, over which the administrative supervision is exercised by the Ministry of Administration; however, the implementation of provisions on citizenship and registers of citizenship is under the jurisdiction of the Ministry of the Interior.

34. The Ministry of Defence keeps records on conscripts in compliance with the Law on Defence. The Republic of Croatia is undergoing a process of computerization of the whole system of records on conscripts.

35. State records of voting rights and personal data of citizens (birth, marriage, death) in the Republic of Croatia are not linked into a central computer system. Computerization of these data has been partially done in government administrative bodies which directly keep them; so far these data have not been mutually linked in the territory of the Republic of Croatia. Connecting these data into a central system has yet to be done, but it will depend on finances.

36. Personal data regarding voting rights, births, marriages and deaths are gathered, processed and used in accordance with the Guidelines for the Regulation of Computerized Personal Data Files (E/CN.4/1990/72). Regulations of the Republic of Croatia governing procedures in keeping records comprise the principles from the Guidelines:

(a) Data to be gathered are stipulated by the law, as well as the way they are processed and the purpose for which they are used (Principle of lawfulness and fairness);

(b) A separate law stipulates that it is the task of the government administrative bodies to check the accuracy and relevance of the data (Principle of accuracy);

(c) The use of the gathered data is stipulated by the law, stating the purpose for which the data can be used and under what circumstances. For example, by being registered in the State records, a person gains the right to documents by which facts on birth, marriage or deaths can be proved. State

registers issue several kinds of documents (transcripts, birth certificates, certificates) by which personal data are proved, depending on the need and request (Principle of the purpose-specification);

(d) Data on voting rights are accessible to the public during the elections while personal data (birth, marriage, death) are under special protection both in terms of getting access to State registers and receiving public documents. Public documents are issued at the request of a person who has a legal interest while the access to State records is allowed to a person to whom these data relate, members of his/her immediate family, adopter or guardian, and other persons only when he/she has legally stipulated legal interest (Principle of interested-person access);

(e) The above registers do not contain data on racial or religious origin, colour, sexual life, political, religious, philosophical or other views nor on membership in a society or trade union, so that they cannot be the basis for any discrimination under the above-mentioned criteria (Principle of non-discrimination);

(f) The law does not provide for the possibility of using the data for exceptional needs which could violate the principles stated in (a) - (e) above.

37. There are special provisions about the security of data. Voting rolls must be kept for five years after their confirmation (voting rolls are confirmed immediately before the elections) while registers of births, marriages and deaths are kept permanently.

38. Computer data are protected from destruction and damage by special project of copying and storing them in a safe place.

39. Unfortunately, in spite of all security measures the Republic of Croatia has no access to registers on temporarily occupied territories. It is not known whether personal data of citizens have been destroyed.

40. EDP security measures against unauthorized use of personal data are the following: a special programme sign for each job; work stations for only one job (access to data allowed only to authorized persons); a certain programme is allocated only the corresponding data structure. However, the Republic of Croatia still lacks legal regulations on the security of information systems, concerning both programme and physical protection measures. Measures of programme protection of information systems require special data protection programmes which would enable full integrity of a databank and which could start functioning immediately in case the system breaks down for any reason.

41. The Ministry of Administration controls the implementation of the law concerning the above-mentioned registers, i.e. registers of births, marriages and deaths and voting rolls, while the Ministry of the Interior controls the implementation of the substantive law concerning the register of citizenship.

42. The Law on the Protection of Personal Data is being drafted and is to be adopted at the end of 1994. It will provide for a mechanism of legal protection of all structured groups of personal data (not only computerized).

43. The proposed Law is based on the principles contained in the Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data of the Organization for Economic Cooperation and Development (Paris, 1980), and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Council of Europe, Strasbourg, 1981). As these principles are also contained in the Guidelines for the Regulation of Computerized Personal Data Files, the proposed Law already contains the principles of points 1 - 9 of the Guidelines.

44. The primary objective of this Law is a legally based protection of personal data (of citizens to which the data refer) and in this connection the establishing of rights, principles, proceedings and conditions concerning the prevention of unauthorized, irregular and unnecessary (excessive) interference in a man's integrity (privacy) in all activities of gathering, processing, storing and using personal data in public and private sphere.

D. Germany

[Original: English]
[9 August 1994]

45. Like many other European States, the Federal Republic of Germany and its Federal Länder have passed data protection laws for their areas of responsibility. In 1970, the Federal Land Hesse was the first entity worldwide to establish a data protection law; the first Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) was passed in 1977. There are data protection laws in all Länder, some of them of the second or their generation. The BDSG, too, was fully amended in 1990.

46. Due to the division of responsibilities by the Basic Law (Grundgesetz) the BDSG regulates data protection within public federal bodies as well as within private bodies, whereas the data protection laws of the Länder contain provisions governing data protection within the public bodies of the respective Land. Some sectoral laws, such as the Code of Social Law, also contain sectoral data protection provisions.

47. Furthermore, the protection of personal data is enshrined in the German Constitution. The Federal Constitutional Court (Bundesverfassungsgericht), in its ruling on the Census Act (Volkszählungsgesetz) of 15 December 1983, acknowledged that the general rights of liberty laid down in article 2, paragraph 1, of the Basic Law in conjunction with article 1, paragraph 1, of the Basic Law include the "right of the individual to determine the use and disclosure of his or her data". Limitations on this right are permissible only in so far as the interest of the general public is overriding and the limitations are based on a clearly defined law which respects the principle of reasonableness.

48. The German data protection legislation more or less anticipated the principles of the United Nations guidelines. Therefore, there has been no genuine need to enact them in German law.

49. The following statements, which refer to the particular principles of the United Nations guidelines, are based on the BDSG. The data protection laws of the Länder, though, provide parallel regulations.

(a) Principle 1 - The German data protection law forbids the use of personal data unless a legal provision provides otherwise or the data subject has given his consent (section 4, subsection 1 of the BDSG);

(b) Principle 2 - Any controller of files is under the obligation to safeguard the protection of personal data through technical and organizational measures (section 9 of the BDSG);

(c) Principle 3 - The Federal Constitutional Court, in the above-mentioned "census ruling", has already established the principles of purpose specification and utilization for the specified purpose. They have been put into practice in section 14 of the BDSG, to name just one provision, which contains an exhaustive catalogue of facts which allow that, for important reasons, data may be used for purposes other than the ones specified (e.g. criminal prosecution, avoidance of danger);

(d) Principle 4 - The German data protection law grants the right of data-subject access (sections 19, 34 of the BDSG) as well as the rights to rectification, erasure and blocking (sections 20, 35 of the BDSG). Pursuant to section 6 of the BDSG these are among the mandatory rights of the data subject, i.e. they cannot be precluded or restricted even if he or she has consented to it (section 6 of the BDSG);

(e) Principle 5 - The special protection of sensitive data is regulated predominantly in sectoral laws;

(f) Principle 6 - The criteria contained in this principle are quite a true reflection of the German laws and Constitution. The individual's right to determine the use of his or her data must constantly be weighed against other constitutional goods and is sometimes outweighed by higher valued goods or goods of the same value;

(g) Principle 7 - The BDSG, in section 9, requires all controllers of files to take technical and organizational measures so as to guarantee the integrity of personal data. A 10-point catalogue containing very concrete instructions is contained in an annex to this provision;

(h) Principle 8 - In the public bodies of the Federation and of the Länder, compliance with data protection provisions are monitored by the Federal Commissioner for Data Protection and by the Land Commissioners for Data Protection of the Länder. They are independent in the exercise of their functions and subject only to law and statutes, like judges. In the case of private bodies, i.e. mainly private companies, control functions are incumbent on the Land supervisory authorities which are bound by instructions and part of the hierarchical administrative structure. However, they are independent of the body to be monitored, as required by Principle 8. In so far as the general penal law (e.g. sections 201 seq of the Penal Code) does not apply

where data protection provisions have been breached, the BDSG (sections 43, 44) and the Land data protection laws make special cases criminal or administrative offences;

(i) Principle 9 - The Federal Republic supports and applies the principle of "reciprocal safeguards" where data are communicated across borders. When construing the relevant legal provisions, the protection level provided by the receiving country is one factor to be weighed so as to assess the interests of the data subject;

(j) Principle 10 - The BDSG covers automated and manual data files, and, in the public sphere, also records, i.e. any document serving official purposes. However, the scope of the BDSG does not cover legal persons. Yet, the protection of data concerning legal persons, these being almost exclusively companies, is derived from the freedom of trade enshrined in article 12 of the Basic Law. In Germany, safeguarding the protection of such data comes under the heading of commercial law in the wider sense, not under that of data protection law.

E. Luxembourg

[Original: French]
[16 September 1994]

50. Since 1979, Luxembourg has had a law regulating the use of computerized personal data. This law was subsequently amended 1/ to conform to the "Guidelines for the regulation of computerized personal data files" (E/CN.4/1990/72), adopted by the General Assembly in its resolution 45/95 of 14 December 1990.

51. By the Act of 19 November 1987, Luxembourg approved the Convention (of the Council of Europe) for the Protection of Individuals with regard to Automatic Processing of Personal Data, done in Strasbourg on 28 January 1981 (ETS No. 108), the only binding international legal instrument in existence to date.

F. Malta

[Original: English]
[3 October 1994]

52. The Government of Malta indicated that all points covered by the Guidelines (E/CN.4/1990/72) are addressed in comprehensive draft legislation currently being subject to Cabinet scrutiny prior to proposal for adoption by the House of Representatives of Malta. This legislation, known as the Information Practices Act, is expected to be in place by mid-1995.

G. Norway

[Original: English]
[23 August 1994]

53. The Government of Norway referred in its reply to the Personal Data Register Act (PDRA) of 9 June 1978 1/ and to the regulations issued in pursuance of this act on 21 December 1978 with amendments of 10 March 1981 1/ which dealt with the principles contained in the guidelines in document E/CN.4/1990/72 as follows:

(a) Principle 1 was covered by PDRA as well as through the work of the Data Inspectorate established under this Act;

(b) Principle 2 was covered by PDRA, section 8;

(c) Principle 3 was covered by PDRA, section 11, paragraph 1, through the work of the Data Inspectorate, and by the Regulations issued pursuant to the Act, sections 1-2, paragraph 2;

(d) Principle 4 was covered by PDRA, section 7;

(e) Principle 5 was covered by PDRA, section 6, paragraph 2;

(f) Principle 6 was covered by PDRA, sections 9 and 6;

(g) Principle 7 was covered by PDRA, sections 8b and 11, through the work of the Data Inspectorate;

(h) Principle 8 was covered by PDRA, sections 2, 5 and 38;

(i) Principle 9 was covered by PDRA, section 36, and by Regulations, chapter 8;

(j) Principle 10 was covered by PDRA, sections 1 and 9.

H. Philippines

[Original: English]
[22 September 1994]

54. The Philippine Government reported that it had instituted certain standards or guarantees, as evidenced by the several existing statutes and cases in jurisprudence, which included the following:

(a) Legal provisions:

(i) The Constitution of the Philippines, in its Art. III, Sec. 3 (1), provides that "the privacy of communication and correspondence shall be inviolable except upon lawful order of the court";

(ii) Republic Act 4200, otherwise known as the "Anti-Wire Tapping Act," prohibits and penalizes the use of an electronic device to overhear any communications for the purpose of obtaining information concerning a certain person;

(iii) The Civil Code of the Philippines, in its Art. 32, penalizes any public officer or employee or any private individual who directly or indirectly impedes or impairs the privacy of communication and correspondence;

(iv) Memorandum-Circular Nos. 78 and 196 (from the Office of the President), promulgate rules governing security of classified matters in government offices, prohibiting the release of information contained in government documents and requiring the government agency to mark a confidential document with the word "Confidential" and the following warning:

"The unauthorized disclosure of information contained in the attached documents, while not endangering national security, would be prejudicial to the interest or prestige of the nation, or any governmental activity or would cause administrative embarrassment or unwarranted injury to an individual or would be of advantage to a foreign nation.";

(v) The Revised Penal Code, in its Art. 228, penalizes any public officer who, without proper authority, shall open or permit to be opened any closed papers, documents, or objects entrusted to his custody. In its Art. 229, the same Code penalizes any public officer who shall reveal any secret known to him by reason of his official capacity or shall wrongfully deliver papers of which he may have charge. Art. 230 also of the same Code penalizes any public officer to whom the secrets of any private individual shall become known by reason of his office, if he shall reveal such secrets;

(b) Philippine jurisprudence

(i) In the case of Valmonte vs. Belmonte, Jr. (170 SCRA 256), the Philippine Supreme Court, on 13 February 1989, ruled that "there can be no doubt that the right to privacy is constitutionally protected";

(ii) In the landmark case of Orfe vs. Mutuc (130 Phil 415, 1968 and 22 SCRA 424), the Philippine Supreme Court, speaking through then Mr. Justice Fernando, stated:

"The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, fully deserving of Constitutional protection. The language of Professor Emerson is particularly apt: 'The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between

> absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the State can control. Protection of this private sector - protection, in other words, of the dignity and integrity of the individual - has become increasingly important as modern society has developed. All the forces of technological age - industrialization, urbanization, and organization - operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and totalitarian society.'".

55. The Philippines believes that the foregoing (legal provisions and Philippine jurisprudence) are sufficient safeguards to enhance the right of a person to his privacy. These are standards essential to the enhanced right to self-determination, as envisioned by the provisions of the United Nations Guidelines for the Regulation of Computerized Personal Data Files. The Guidelines, when strictly adopted as a means of achieving the ends of the foregoing laws and jurisprudence, will foster and strengthen the integrity of the basic rights of the Filipinos as they commune with the entire human community.

56. The Philippines therefore finds no reason not to support the revised version of the United Nations Guidelines for the Regulation of Computerized Personal Data Files. It is for this reason and along these lines that the Philippine Commission on Human Rights has adopted the Guidelines on the Use and Management of Computerized Personal Data Files. 1/

I. Saudi Arabia

[Original: English]
[30 May 1994]

57. The Government of Saudi Arabia submitted the following comments:

> "Computerized personal data files" on citizens are the property of the State. Therefore, the "Guidelines" for such a device are not applicable to Saudi Arabia.

J. Spain

[Original: Spanish]
[15 July 1994]

58. The Government of Spain submitted copies of the following legislative acts:

(a) Organization Act No. 5/1992 of 29 October 1992 regulating the automated processing of personal data (B.O.E., 31 October 1992); 1/

(b) Royal Decree No. 428/1993 of 26 March 1993 approving the Statutes of the Data Protection Agency; 1/

(c) Royal Decree No. 1332/1994 of 20 June 1994 developing certain aspects of Organization Act No. 5/1992 of 29 October 1992 regulating the automated processing of personal data. 1/

K. Sweden

[Original: English]
[25 August 1994]

59. The Government stated that Sweden had a long tradition of protecting personal privacy with regard to computerized data files. The Swedish Data Protection Act of 1973 was the first national Act of its kind in the world. (A copy of the Act as amended with effect from 1 July 1992 was enclosed). 1/ In 1982 Sweden was the first country to ratify the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108).

60. The Act of 1973 regulates the use of personal data files. "Personal data files" are such files, lists and other notes in which automatic data processing (ADP) is used and which contain personal data on an identifiable physical person. Manual files are not covered by the Act.

61. The Act stipulates that there has to be a controller responsible for every automated personal data file. The controller of the file is the natural person, agency or legal person who decides about the information in the file and can, when need be, modify the file or transform the contents of the file into a readable form.

62. According to the provisions of the Data Protection Act of 1973, anyone who wishes to create an automated personal data file is obliged to notify the Swedish Data Protection Agency (Datainspektionen) and obtain a licence. Such a licence gives the controller of the file the right to create and operate an unlimited amount of files relating to the specific licence obtained.

63. Apart from the licence requirement the Act of 1973 contains provisions regarding certain sensitive personal data files, for which the special permission of the Agency is needed. Among the special categories of personal data, for which particular safeguards are provided, are data relating to criminal convictions or detentions based on administrative decisions, data concerning health or sexual life or revealing racial origin, political opinions, religion or other beliefs. Permission is also needed to maintain files containing qualifying statements of persons. Files containing information on persons without a specific connection to the controller also require permission. If there is a specific connection between the controller of the file and the person registered, the files are exempt from this permission requirement. Examples of such privileged files are files with information on clients, customers, members of organizations, etc. or employees. "Cross-matching" of files, i.e. transfer of data from one file to another, and joint processing of several personal data files also require the permission of the Agency.

64. The Data Protection Agency can grant permission only if there is no reason to believe that the automatic data processing of the personal data file would unduly infringe the registered person's right to privacy.

65. The transfer of a file to another country also needs the permission of the Agency, unless the transfer takes place to a country which has signed the Council of Europe Convention of 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data. The permission can be granted only if the Agency can expect that such a transfer will not infringe the registered person's right to privacy.

66. There are also certain general provisions regarding the storage of personal data files in archives.

67. The Data Protection Agency supervises the controllers of the files and the general application of the Act.

68. If ADP of personal data has infringed or could be expected to unduly infringe the right to privacy, the Agency can set specific conditions for the ADP or, if it is not possible to revise the contents of the file in any other way, prohibit the controller from processing the file or withdraw permission once granted.

69. Decisions of the Data Protection Agency are subject to review by the Government.

70. In 1993 a Commission presented a proposal for a new Data Protection Act. Due to the uncertainty of the future data protection level in Europe the Government has decided not to present a proposal for a new Act at the moment.

71. Meanwhile the Government on 14 April 1994 presented a Bill to the Parliament with amendments to the Data Protection Act of 1973 in order to reduce the system of special permissions and increase the supervision of the Data Protection Agency. Among other things the Bill also contains a proposal that the decisions of the Data Protection Agency shall be appealed to a court of justice instead of as present to the Government. It is proposed that the amendments to the Data Protection Act shall enter into force on 1 January 1995.

L. United Kingdom of Great Britain and Northern Ireland

[Original: English]
[15 September 1994]

72. The Government reported that the United Kingdom data protection law takes account of the general principles set out in the United Nations guidelines. The Data Protection Act 1984 gives rights to individuals about whom information is processed automatically (i.e. on computer). The individual may find out what information is held about him, challenge its accuracy and in certain circumstances claim compensation. Those who hold computerized personal information must register with the Data Protection Registrar and follow specified principles governing the way in which they obtain, record and use their data.

73. The key features are as follows:

(a) The Act applies to all personal data which are computerized or in a form suitable for automatic processing, except where processed at home for domestic purposes or by companies for pay, pensions, accounts, purchases or sales purposes (but not personnel records or marketing). There are also exceptions where the information is solely for distribution of articles or information to data subjects by incorporated members' clubs; for data which the data user is required by law to make public (e.g. the Electoral Register); or where data are held for national security purposes (as determined by government ministers);

(b) All data users who are not exempt must register: information about the type of data which they hold; the purposes for which the data are used; the sources from which the data came; the people to whom the data may be disclosed and any overseas countries to which data may be transferred;

(c) Data users must comply with data protection principles. The principles require personal data to be collected and processed fairly and lawfully; held only for the lawful purposes described in the register entry; used only for those purposes, and be disclosed only to people described in the register entry. Data must be adequate, relevant and not excessive for the purpose for which they are held; be accurate and, where necessary, kept up to date; held no longer than is necessary for the registered purpose; and surrounded by proper security;

(d) The Registrar may serve three types of notice to enforce compliance with the principles: an enforcement notice specifying action to take; a de-registration notice cancelling all or part of a register entry (it is an offence to hold data not covered by a valid entry); and a transfer prohibition notice which prevents transfer overseas;

(e) Data subjects (individuals, not organizations) may seek compensation through the courts for damage caused by loss, unauthorized destruction or unauthorized disclosure of personal data, or for damage caused by inaccurate data. The data subject may also complain to the Registrar, or apply to the courts for correction or deletion of data. The subject may also, by a written request and fee, obtain from any data user a copy of personal information held about them (except, for example, where such subject access would be likely to prejudice the prevention or detection of crime). He may complain to the Registrar or apply to the courts for an order if access is not given within 40 days;

(f) If a data subject considers there has been a breach of one of the principles or any provision of the Act he may complain to the Registrar, who must consider the complaint if it is substantial and made without undue delay. The Registrar can seek to resolve it informally, prosecute or serve a notice on a data user;

(g) A data user may disclose information about an individual, provided the destination has been properly registered in the register entry, or there is a "non-disclosure exemption" (e.g. disclosure required by law or made with the data subject's consent);

(h) The Registrar reports directly to Parliament. He holds the Register of data users and computer bureaux, makes it publicly available, and disseminates information on the Act and how it works. The Registrar also promotes compliance with the principles, and where appropriate encourages the development of codes of practice. He considers complaints about breaches of the principles or Act and, where appropriate, prosecutes or serves notices;

(i) Data users or computer bureaux may appeal to a Data Protection Tribunal against decisions made by the Registrar to refuse registration applications, to serve enforcement notices, to de-register, or to serve transfer prohibition notices. The Tribunal can overturn the Registrar's decision. On questions of law further appeal may be made to the High Court.

74. Copies of some guidelines prepared by the Data Protection Registrar, which explain the 1984 Act in more detail, were enclosed. 1/

M. Yugoslavia

[Original: English]
[14 November 1994]

75. The Government of the Federal Republic of Yugoslavia submitted the following information.

76. The eighth session of the two Councils of the Federal Assembly held on 2 October 1990 adopted the Law on the Ratification of the Convention on the Protection of Persons against Automatic Personal Data Processing. In this way, the Federal Republic of Yugoslavia took over the obligation to regulate, in its domestic legislation, the matter of the protection of personal data contained in computerized files.

77. Proceeding from article 33, paragraph 4, of the Constitution of the Federal Republic of Yugoslavia, according to which the federal law regulates the collection, processing, use and protection of personal data, the Federal Ministry of Human and Minority Rights and the Federal Informatics Institute have prepared a draft law on the protection of personal data approved at the 164th meeting of the Federal Government on 21 April 1994. The draft provisions are in accordance with the provisions of the said Convention. The draft law is now in the procedure of the Federal Assembly.

78. The draft law on the protection of personal data includes all the principles provided by the Guidelines, except the status of personal data files handled by governmental international organizations.

Following are the principles contained in the Guidelines and the draft law:

(a) Principle of lawfulness and fairness - articles 1 and 2 of the draft law;

(b) Principle of accuracy - article 12 of the draft law;

(c) Principle of the purpose-specification - article 2 of the draft law;

(d) Principle of interested-person access - articles 11 and 12 of the draft law;

(e) Principle of non-discrimination - article 20 of the draft law;

(f) Power to make exceptions - article 13 of the draft law;

(g) Principle of security - article 8 of the draft law;

(h) Supervision and sanctions - articles 21 to 25 and 27 of the draft law;

(i) Transborder data flows - article 26 of the draft law.

III. INFORMATION SUBMITTED BY INTERGOVERNMENTAL ORGANIZATIONS

A. Council of Europe

[Original: English]
[12 August 1994]

79. The European Commission of Human Rights of the Council of Europe indicated that the Commission had been requested to deal, under article 8 of the European Convention of Human Rights, with the use of personal data files by different national authorities. However, there were very few decisions on computerized data files. Enclosed was the decision of the Commission of 11 December 1985 No. 10473/83 (Tom Lundvall vs. Sweden). 1/

B. Interpol

[Original: French]
[9 August 1994]

80. The International Criminal Police Organization (Interpol) submitted the following information:

"OBSERVANCE BY ICPO-INTERPOL OF THE GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES

Introduction

The principle of the protection of data kept by the General Secretariat of ICPO-Interpol is established in a treaty (Headquarters Agreement and Exchange of Letters of 1982) between the Government of the French Republic and the Organization, and in internal regulations entitled 'Regulations concerning international police cooperation and the internal control of ICPO-Interpol files'. The texts of these three legal instruments, together with the Constitution of the Organization, are appended 1/ as they constitute the legal

framework governing the implementation of the guidelines set out in United Nations document E/CN.4/1990/72, as incorporated within the Organization's legal provisions.

1. Derogation from the domestic law of the headquarters country

The 1982 Headquarters Agreement, which entered into force on 14 February 1984, declares the headquarters, archives and correspondence of the Organization to be inviolable (arts. 4, 7 and 9). It further provides that the files (of Interpol) shall be subject to internal control exercised by the Organization in accordance with the general rules established by Exchange of Letters with the Government of the French Republic (art. 8).

This Exchange of Letters makes the files kept by the General Secretariat of ICPO-Interpol subject to the control of an independent committee for whose establishment the Organization is responsible. Its composition and operation and the principle underlying the controls it is required to execute are forcefully and clearly defined in the provisions of the Exchange of Letters.

It therefore follows that the ICPO-Interpol files are covered by the provisions of the Headquarters Agreement and exempted from supervision by the National Commission on Computerization and Freedoms (CNIL), which is a French body responsible for ensuring compliance with the 1978 Act on the protection of data in France.

2. Designation of the authority with statutory competence to supervise the proper implementation of the guidelines

The Organization has honoured its commitment set out in the Exchange of Letters through the adoption of the 'Regulations concerning international police cooperation and the internal control of ICPO-Interpol files'. These regulations, hereafter referred to as the 'Cooperation regulations', constitute the act by means of which the Organization established the ICPO-Interpol Internal Files Control Committee.

This Committee is a subsidiary body of the Organization, which has designated it as the authority statutorily competent to supervise the implementation of the rules adopted by ICPO-Interpol with regard to the protection of personal data.

The establishment of this Committee, whose composition and operation are laid down in articles 15 et seq. of the Cooperation Regulations, therefore corresponds to the recommendations made under section B in document E/CN.4/1990/72 concerning international organizations.

It should be noted that Mr. Louis Joinet, judge/technical adviser in the Office of the French Prime Minister at the time of the negotiation of the Headquarters Agreement between ICPO-Interpol and France and rapporteur of the United Nations Commission on Human Rights, referred to this Committee as a body which could serve as a model for the supervision of the files of many international organizations having their headquarters in France.

3. Content of the guidelines adopted by ICPO-Interpol

ICPO-Interpol has incorporated the guidelines applicable to personal data files kept by governmental international organizations in its internal legislation in the following manner.

Principle of lawfulness and fairness (No. 1)

This principle is established by the Constitution of ICPO-Interpol, in particular in article 2, which sets out the main responsibilities of the Organization, establishes its area of competence, and makes express reference both to the spirit of the Universal Declaration of Human Rights and to compliance with the laws existing in the various States dealing with Interpol through the National Central Bureaux which form part of their national authorities.

Pursuant to this principle, article 1, paragraph 2, of the Cooperation Regulations stipulates that their purpose is to protect against any abuse police information processed and communicated within the international police cooperation system established by ICPO-Interpol, in particular with a view to preventing any infringement of the rights of individuals.

Observance of the principle of lawfulness implies, in turn, observance of two fundamental legal provisions in the Interpol system. These are articles 5 (3) and 3 (3) of the Cooperation Regulations.

Article 5 (3) of these Regulations provides that the General Secretariat is only the depositary of the police information transmitted to it by national police authorities. It follows from this provision that the national police authorities (who are the principal source of information for Interpol) are required to verify the legitimacy and legality of the communication of the information they wish to transmit to the Organization.

Once the information has been communicated to the General Secretariat, its processing, registration and communication are subject to the Organization's internal rules. Thus, article 3 (3) of the Cooperation Regulations provides that the processing of police information by the General Secretariat ... shall not be subject to any national legislation. It shall be effected in accordance with the provisions of these Regulations and the agreements concluded with the Headquarters State.

Principle of accuracy (No. 2)

Several provisions of the Cooperation Regulations establish this principle as an obligation incumbent both on the General Secretariat and on the country of origin of the information deposited with the General Secretariat. These provisions are to be found in articles 5 (2), 6 (2), 6 (3), 7 (5) and 9 (4) of the Cooperation Regulations.

The obligation to keep accurate information gives rise not only to an obligation to update, but also to an obligation to eliminate information. Thus, article 5 (5) of the Cooperation Regulations provides that the destruction, by the General Secretariat, of police information considered to

be outdated on the basis of certain general criteria shall be determined by specific regulations approved by the General Assembly. These regulations were adopted in 1987.

Principle of purpose-specification (No. 3)

In accordance with article 3 (4) of the Cooperation Regulations, the processing of police information by the General Secretariat is effected with the aim of the prevention and punishment of ordinary criminal offences within the meaning of article 2, paragraph (b), of the Constitution and not covered by article 3 of the Constitution, in the interest of the investigations concerning them, for the purposes of finding missing persons and identifying bodies.

This principle is also established in article 22 (b) of the Cooperation Regulations, which make the Internal Files Control Committee responsible for ensuring that the information kept by the General Secretariat is registered and processed for specific purposes.

The personal data compiled and processed by the General Secretariat therefore serve police purposes. It is for this reason that the Organization has derogated from the principle of publicity or information relating to the person concerned before the data are used or transmitted to the competent police authorities, in accordance with principle No. 6 establishing the power to make exceptions.

Principle of interested-person access (No. 4)

This principle is laid down in article 23 of the Cooperation Regulations, which provides for the possibility for persons who may be interested to request the Control Committee to verify information concerning them. The Committee will then notify the person making the request that this verification has been undertaken, without revealing the content of the information kept. What is involved therefore is a right of indirect access by individuals to the Organization's police files.

This indirect access to police files is justified by the difference in purpose between a national police file and an international police file managed by the Organization acting as depositary for the information entrusted to it. In fact, it is not for the Organization to decide whether the disclosure of police information may harm the public order of a member State or jeopardize cooperation between two or more member States.

Thanks to this system established by the Organization, many persons who do not have the right of even indirect access to the police files of their own country can exercise this right at the international level.

Principle of non-discrimination (No. 5)

Subject to the need to identify a person wanted at the international level and the need to describe acts constituting ordinary criminal offences,

this principle is established by article 3 of the Organization's Constitution, which forbids it to intervene in cases of a political, military, religious or racial nature.

Power to make exceptions (No. 6)

The provisions adopted by the Organization with regard to the protection of data correspond to the guidelines set out in document E/CN.4/1990/72, subject to such exceptions or adaptations as may be justified by the specific nature of the activities of ICPO-Interpol, these adaptations being authorized under section B and principle 6 of section A of document E/CN.4/1990/72 providing for the "power to make exceptions" to certain principles in order to protect security, public order, and the rights and freedoms of others.

Furthermore, the Organization performs a humanitarian role in the context of searches for missing persons and the identification of bodies. The Organization's functions in this area simply represent an international extension of the humanitarian role of the police at the national level.

Lastly, in accordance with article 3, paragraphs 3 and 4, of the Cooperation Regulations, all police data may also be used for the purposes of internal management, for scientific research and publications, and for the pursuit of any other legitimate goal, provided that the identification of persons who may thereby be concerned is rendered impossible.

Principle of security (No. 7)

Article 1, paragraph 2 (cited above), of the Cooperation Regulations, which prohibits any improper use of police information, and article 4 of the Regulations establish this principle of security. Thus, article 4 of the Regulations provides that the General Secretariat shall take the necessary precautions to preserve the secrecy and security of police information and prevent this information from being processed or communicated in an unlawful or improper manner. This article further provides that the personnel of the General Secretariat are required to observe confidentiality. This obligation of confidentiality also extends to the members of the Control Committee under article 19 of the Regulations.

Sophisticated computerized protection measures and strict administrative procedures have also been developed by the General Secretariat to protect data against any interference or unauthorized access.

Supervision and sanctions (No. 8)

In accordance with article 22 of the Cooperation Regulations, the main responsibility of the ICPO-Interpol Internal Files Control Committee is to ensure that personal information contained in Interpol files is obtained, processed and preserved in accordance with the principles enunciated in this document.

In order to carry out its overall supervisory responsibilities, the Commission has direct access to all the Organization's files and has a right of investigation which it may invoke vis-à-vis the General Secretariat. It

may also consult the Organization's Executive Committee and the police authorities of the country of origin of information subject to its verification. With a view to exercising this overall supervisory responsibility, the Commission undertakes verification either at the request of a private individual or ex officio by examining police files which it selects on a random basis.

The Committee may request the modification or destruction of information kept by the General Secretariat in accordance with article 24 (3) of the Cooperation Regulations. The results of its supervision and its investigations are notified to the Executive Committee in order that the competent organs may make the necessary amendments in accordance with article 25 of the Cooperation Regulations.

Transborder data flows (No. 9)

The circulation of information between the General Secretariat and the police authorities of States members or other authorized bodies is governed both by the principles set out above and by a number of specific provisions of the Cooperation Regulations (arts. 5, 7, 8 and 9) which make the communication of police information to police authorities or other national or international bodies subject to strict conditions.

Field of application (No. 10)

Two kinds of personal files are kept by the General Secretariat of the Organization: police files and administrative files.

The principles set out above apply to manual or automated police files (Criminal Information System).

The administrative files comprise files on the Organization's personnel and persons who have official contacts with it. These files are not subject to the same legal rules as those governing the police files. This does not, however, prevent the Organization from observing the guidelines set out in document E/CN.4/1990/72, subject to their adaptation to the needs of the proper functioning of the Organization and verification by the ICPO-Interpol Internal Files Control Committee.

To sum up, the information kept by the General Secretariat on its staff and its collaborators or visitors is compiled in a lawful manner on the basis of statements by the persons actually concerned and public sources (civil or commercial registers, national authorities, international bodies, etc.) and taking account of updates by the persons concerned or the competent departments of the General Secretariat, after verification of their accuracy. These administrative files are used for management, accounting, social welfare and administrative purposes and any other purpose consistent with the aims and objectives of the Organization as enunciated in its Constitution and internal regulations.

The Constitution and the Staff Regulations therefore incorporate the principles of the international civil service while at the same time adapting certain principles set out in document E/CN.4/1990/72. They authorize direct access by personnel to their files. The data concerning personnel are confidential and are used only for management and administrative purposes. Any unauthorized access or access which is not justified by professional needs is forbidden. Violation of these principles may give rise to disciplinary procedures, subject to supervision by the ILO Administrative Tribunal."

Note

1/ Available for consultation in the files of the secretariat.

Annex

GUIDELINES CONCERNING COMPUTERIZED PERSONAL DATA FILES

The procedures for implementing regulations concerning computerized personal data files are left to the initiative of each State subject to the following orientations:

A. Principles concerning the minimum guarantees that should be provided in national legislations

1. PRINCIPLE OF LAWFULNESS AND FAIRNESS

Information about persons should not be collected or processed in unfair or unlawful ways, nor should it be used for ends contrary to the purposes and principles of the Charter of the Untied Nations.

2. PRINCIPLE OF ACCURACY

Persons responsible for the compilation of files or those responsible for keeping them have an obligation to conduct regular checks on the accuracy and relevance of the data recorded and to ensure that they are kept as complete as possible in order to avoid errors of omission and that they are kept up to date regularly or when the information contained in a file is used, as long as they are being processed.

3. PRINCIPLE OF THE PURPOSE-SPECIFICATION

The purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure that:

(a) All the personal data collected and recorded remain relevant and adequate to the purposes so specified;

(b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified;

(c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.

4. PRINCIPLE OF INTERESTED-PERSON ACCESS

Everyone who offers proof of identity has the right to know whether information concerning him is being processed and to obtain it in an intelligible form, without undue delay or expense, and to have appropriate rectifications or erasures made in the case of unlawful unnecessary or inaccurate entries and, when it is being communicated, to be informed of the addressees. Provision should be made for a remedy, if need be with the supervisory authority specified in principle 8 below. The cost of any

rectification shall be borne by the person responsible for the file. It is desirable that the provisions of this principle should apply to everyone, irrespective of nationality or place of residence.

5. PRINCIPLE OF NON-DISCRIMINATION

Subject to cases of exceptions restrictively envisaged under principle 6, data likely to give rise to unlawful or arbitrary discrimination, including information on racial or ethnic origin, colour, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.

6. POWER TO MAKE EXCEPTIONS

Departures from principles 1 to 4 may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as, inter alia, the rights and freedoms of others, especially persons being persecuted (humanitarian clause) provided that such departures are expressly specified in a law or equivalent regulation promulgated in accordance with the internal legal system which expressly states their limits and sets forth appropriate safeguards.

Exceptions to principle 5 relating to the prohibition of discrimination, in addition to being subject to the same safeguards as those prescribed for exceptions to principles 1 and 4, may be authorized only within the limits prescribed by the International Bill of Human Rights and the other relevant instruments in the field of protection of human rights and the prevention of discrimination.

7. PRINCIPLE OF SECURITY

Appropriate measures should be taken to protect the files against both natural dangers, such as accidental loss or destruction and human dangers, such as unauthorized access, fraudulent misuse of data or contamination by computer viruses.

8. SUPERVISION AND SANCTIONS

The law of every country shall designate the authority which, in accordance with its domestic legal system, is to be responsible for supervising observance of the principles set forth above. This authority shall offer guarantees of impartiality, independence vis-à-vis persons or agencies responsible for processing and establishing data, and technical competence. In the event of violation of the provisions of the national law implementing the aforementioned principles, criminal or other penalties should be envisaged together with the appropriate individual remedies.

9. TRANSBORDER DATA FLOWS

When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the

territories concerned. If there are no reciprocal safeguards, limitations on such circulation may not be imposed unduly and only in so far as the protection of privacy demands.

10. FIELD OF APPLICATION

The present principles should be made applicable, in the first instance, to all public and private computerized files as well as, by means of optional extension and subject to appropriate adjustments, to manual files. Special provision, also optional, might be made to extend all or part of the principles to files on legal persons particularly when they contain some information on individuals.

B. Application of the guidelines to personal data files kept by governmental international organizations

The present guidelines should apply to personal data files kept by governmental international organizations, subject to any adjustments required to take account of any differences that might exist between files for internal purposes such as those that concern personnel management and files for external purposes concerning third parties having relations with the organization.

Each organization should designate the authority statutorily competent to supervise the observance of these guidelines.

Humanitarian clause: a derogation from these principles may be specifically provided for when the purpose of the file is the protection of human rights and fundamental freedoms of the individual concerned or humanitarian assistance.

A similar derogation should be provided in national legislation for governmental international organizations whose headquarters agreement does not preclude the implementation of the said national legislation as well as for non-governmental international organizations to which this law is applicable.
