UNITED
NATIONS

E

Economic and Social
Council

Distr.
GENERAL

E/CN.4/1997/67
23 January 1997

ENGLISH
Original: ARABIC/ENGLISH/
FRENCH/SPANISH

COMMISSION ON HUMAN RIGHTS
Fifty-third session
Item 12 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 1995/114

CONTENTS

## Introduction

1. In its decision 1995/114 of 8 March 1995, 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, and taking note of the report of the Secretary-General prepared pursuant to Commission decision 1993/113 (E/CN.4/1995/75), decided:

(a) To request States and intergovernmental, regional and non-governmental organizations to cooperate fully with the Secretary-General by providing him with any relevant information on the application of the guidelines;

(b) To request the Secretary-General to continue to ensure the implementation of the guidelines in the United Nations system;

(c) To request the Secretary-General to report to the Commission at its fifty-third session:

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

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

2. Pursuant to that decision, the Secretary-General, on 6 June 1996, addressed requests to United Nations organs, bodies, regional commissions, specialized agencies and related organizations 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 10 December 1996, replies had been received from the following United Nations organs, bodies and specialized agencies: Crime Prevention and Criminal Justice Division, Department of Humanitarian Affairs, Economic Commission for Europe, Economic Commission for Latin America and the Caribbean, United Nations Environment Programme, United Nations Population Fund, World Food Programme, International Atomic Energy Agency, International Labour Organization, International Monetary Fund, International Telecommunication Union, United Nations Educational, Scientific and Cultural Organization.

5. The following Governments have submitted information: Argentina, Austria, Croatia, Estonia, Germany, Libyan Arab Jamahiriya, Luxembourg, Mauritius, Mexico, Philippines, San Marino, Sweden, United Kingdom of Great Britain and Northern Ireland and Uruguay.

6. A reply was received from one intergovernmental organization: the Organization of American States indicated that it was unable to provide the requested information.

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. Of the 33 various United Nations organs, bodies, regional commissions, specialized agencies and related organizations which were addressed, only 12 have replied.

10. The Department of Humanitarian Affairs, the Economic Commission for Latin America and the Caribbean and the International Telecommunication Union stated that they had no relevant information to submit or comments to offer with regard to the issue in question.

11. The Economic Commission for Europe (ECE) stated that there was no activity in ECE to which the decisions of the Commission on Human Rights applied, as ECE statistical files were either anonymous or aggregated.

12. The United Nations Environment Programme indicated that its practice was in line with the provisions contained in the guidelines for the regulation of computerized personal data files.

13. The International Atomic Energy Agency stated that the provisions of its Administrative Manual, section 8, dealing with protection of personnel confidential information, were consistent with the guidelines for the regulation of computerized personal data files adopted by the General Assembly.

14. The International Monetary Fund (IMF) also indicated that the procedure concerning and access to personal data files in IMF appeared to be in close conformity with the guidelines.

15. The United Nations Educational, Scientific and Cultural Organization confirmed that it was adhering to the guidelines on the maintenance of personal data files.

16. The United Nations Population Fund (UNFPA) indicated that all UNFPA personnel matters were administered by UNDP and thus, it followed United Nations/UNDP guidelines, which reflected the principles outlined in document E/CN.4/1990/72 and General Assembly resolution 45/95.

17. The World Food Programme (WFP) submitted the following statement:

> “The computerized personal data of staff directly employed by WFP are kept by the United Nations Food and Agriculture Organization (FAO) also based in Rome, with whom we share a common computerized personnel

system (Persys). FAO has control over and responsibility for this Persys. Staff in the Human Resources of WFP have restricted access to the computerized files for WFP staff only.

"To the best of our knowledge this FAO/Persys is meeting all the guidelines mentioned in document E/CN.4/1990/72 of 20 February 1990."

18. The Crime Prevention and Criminal Justice Division (United Nations Office at Vienna) submitted the following information:

"1. The Division in its activities frequently refers to the 'Guidelines'. Examples involve their inclusion in the sales publications:

(a) 'Guide to Computerization of Information Systems in Criminal Justice' (ST/ESA/STAT/SER.F/58, United Nations publication, Sales No. E.92.XVII.6, p. 155), prepared jointly by the Statistics Division at Headquarters and our Division;

(b) 'United Nations Manual on the Prevention and Control of Computer-Related Crime' (International Review of Criminal Policy Nos. 43 and 44/1994, ST/ESA/SER.M/43-44, United Nations publication, Sales No. E.94.IV.5, para. 138).

"2. References to the 'Guidelines' were also made in the working papers prepared by the Division for the Eighth and Ninth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, held in 1990 and 1995, respectively. In particular, they are contained in documents:

(a) A/CONF.144/14, Computerization of the administration of criminal justice, para. 12;

(b) A/CONF.169/6, Criminal justice and police systems: management and improvement of police and other law enforcement agencies, prosecution, courts and corrections; and the role of lawyers, para. 89.

"2. In its training activities for the criminal justice professionals, particularly implemented in the developing world, experts requested by the Division, and its own staff, inform those professionals about the role of privacy in handling manual and computerized personnel files of alleged offenders and convicts, in line with the 'Guidelines'. Most recently the Division covered the subject of related privacy protection issues at the interregional training course on the computerized 'United Nations Crime and Justice Information Network: Providing Data to and from Developing Countries', organized under the United Nations auspices by the Government of Republic of Korea (Seoul, 9-13 September 1996).

"3. Finally, during various informal consultations with specialists dealing with the question of computer-related crime, and from the perspective of the Division, it felt that at the level of

domestic criminal justice administration, 'Guidelines' may be useful, if their principles could be applied to the two universal and current tendencies:

(a) Increasing danger of organized crime and terrorist acts;

(b) Very dynamic progress in the area of new technologies in information processing.

"4. These two tendencies focus on the operations of criminal justice systems and influence the role of law enforcement (principles 1 through 4 emphasizing collection of data in lawful and fair ways) at the possible cost of protection of privacy (principle 6 dealing with 'power to make exceptions').

"5. In order to strengthen lawful and fair collection of data, and ensure the implementation of the 'Guidelines' cross-nationally, it might be useful to consider reviewing trends in at least two areas:

(a) Whether after 1990 (year of adopting the 'Guidelines') countries have enacted legislation concerning data protection;

(b) Whether there exists a practice of informing the public which electronic criminal justice databases are established and managed (advanced visual recognition systems/closed-circuit television, computerized face recognition, national DNA databases containing genetic fingerprints of alleged offenders, intelligent vehicle and highway tracking systems, ID and other smart cards facilitating various personal transactions)."

19. The International Labour Organization (ILO) submitted the following information:

"As concerns the application of the Guidelines inside the International Labour Office, the ILO has not as yet established computerized personal files as such. These files are still on hard copy and are handled manually. However, the Office is introducing a personnel information system (PERSIS) which has different data banks which are computerized. PERSIS is based on the Integrated Management Information System (IMIS) developed by the United Nations Secretariat in New York, and it is assumed that IMIS was developed in conformity with the Guidelines.

"As regards the principles cited in these Guidelines, ILO practices conform completely:

Principle of lawfulness and fairness: compliance;

Principle of accuracy: Continuous activity to clean and update the database;

Principle of purpose-specification: All data elements in IMIS are directly related to personnel and payroll administration requirements, and no unjustified data elements are included;

Principle of interested-person access: compliance;

Principle of non-discrimination: compliance;

Power to make exceptions: compliance;

Principle of security: The database server is highly protected within the ILO network and the ILO has just installed a very strict firewall to protect against unauthorized access to ILO files;

Supervision and sanctions: compliance;

Transborder data flows: compliance;

Field of application: compliance."

20. The ILO also referred to the Meeting of Experts on Workers' Privacy, which was scheduled to take place from 1 to 7 October 1996 in Geneva. This meeting was expected to discuss a draft code of practice on the protection of workers' personal data and other possible ILO action. The draft guidelines deal with any use of personal data, including collection, storage and communication.

## II. INFORMATION RECEIVED FROM STATES

### Argentina

[Original: Spanish]
[22 August 1996]

1. Following its reform in August 1994, the Constitution now provides, in article 43, paragraph 3, for the action of amparo to be brought by any person to find out what data relating to him or her are contained in public records or data banks, or private ones intended to provide information, and, if the data are false or involve any form of discrimination, to require the data to be deleted, corrected, kept confidential or updated, as well as to know the purpose for which they have been collected.

2. This constitutional provision is a positive response to the guidelines adopted by the General Assembly of the United Nations in its resolution 45/95 of 14 December 1990 and to decision 1995/114 adopted by the Commission on Human Rights on 8 March 1995. Among the principles taken as a basis for the constitutional provision, it is important to note the principles of purpose-specification (para. 3), interested-person access (para. 4), non-discrimination (para. 5), the establishment of supervision (para. 8) and the field of application for public and private records (para. 10).

3. As regards legislative action in this sphere, 18 bills have been put before the National Congress, of which to date only one is half-way towards adoption, having been passed by the Chamber of Deputies of the Congress on 5 June 1996.

4. This bill embodies the guidelines as a whole, making exceptions to their application in conformity with the principle set forth in paragraph 6. In addition, it clearly defines the terms employed to avoid any inconsistencies between terms that might be prejudicial to the full application and effectiveness of the guidelines.

5. As regards the implementing authority, article 5 of the bill creates a Bicameral Commission on Monitoring of Data Protection, within the National Congress, for the purpose of safeguarding and protecting the rights covered by the proposed law.

6. Mention should be made of article 11 of the bill, which requires certain personal data to be especially protected: (i) opinion, race, religion, personal habits and sexual behaviour; (ii) state of health (in this respect, article 12 makes an exception for relevant information to be supplied to health-care and professional centres about persons receiving counselling or treatment at them), personal assets and tax liabilities, except for reasons connected with the general welfare and by provision of law or with the consent of the person concerned; (iii) data relating to criminal proceedings or administrative infractions, which may only be included in records or data banks belonging to the competent public administrations, subject in all cases to their respective regulations.

7. The bill provides that personal data may be disclosed only with the prior consent in writing of the person concerned - which can always be withdrawn - and, at the same time, stipulates that such consent is null and void if it is not clearly specified for what purpose it was given (art. 15). The person's consent will not be required in the cases specifically provided for by the bill for purposes connected with the general welfare, such as the effective administration of justice and public health.

8. Data transmitted to other countries and to international or supranational organizations shall be subject to the same protection as personal data within the Republic.

9. Persons about whom information is contained in the files have the following rights: (i) to challenge any administrative act or private decision founded solely upon an appraisal made of them as a result of the processing of personal data; (ii) to be informed of the existence of the records or data banks, their purpose and the identity of those responsible for them; (iii) to request and obtain the personal information contained in the records or data banks without charge of any kind; and (iv) to correct, delete or conserve the personal data.

10. Regarding the enforcement of rights, the bill provides for a summary proceeding to establish liability, and also determine compensation, for damage or injury caused to the property or rights of the person concerned as a result of the information stored. Such action will be taken under the summary

proceeding and will not preclude the institution of the action of amparo, as provided for by the Constitution and consonant with Act No. 16.986, for whose application the National Code of Civil Procedure provides in article 321 for a streamlined procedure.

11. In respect of persons responsible for records or data banks, the bill furthermore provides - without prejudice to any liability for damage or injury caused to the person affected and to any criminal sanctions to which the offences committed may have given rise - for the sanctions of a caution, suspension or fine, and elimination or closure of the records or data banks, by the Ombudsman, who, in accordance with the regulations to be issued by the Bicameral Commission created under this same law, will be the implementing organ.

12. In accordance with the last article of the bill, the provinces are invited to create their own provincial data bank registers and appoint their own implementing organs; at the same time, the bill provides that the absence of procedural rules governing the matter shall not prevent action from being taken under the streamlined procedure provided for in article 43 of the National Constitution.

13. The preceding paragraphs represent a synopsis of the advances made by the Argentine Republic in this sphere. The full text of the bill described above was attached.*

## Austria

[Original: English]
[11 September 1996]

1. The Austrian Data Protection Act, Federal Law Gazette No. 565/1978 (Datenschutzgesetz - DSG) provides for all the principles of the United Nations “Guidelines for the regulation of computerized personal data files”. In particular, the concepts of purpose-specification (principle 3), as well as lawfulness and fairness (principle 1) and the power to make exceptions for special reasons only (principle 6), are the foundations of data protection in Austria, as can be seen from sec. 1 DSG.

2. Principle 5 is covered by article 6 of the European Council's “Convention for the protection of individuals with regard to automatic processing of personal data”, which was ratified by Austria in 1988 (Austrian Federal Law Gazette No. 317/1988), and applied by the relevant authorities ever since.

3. Following the EU Directive 46/95/EC, liberalization of transborder data flows (principle 9) with regard to other EU member States is to be expected soon.

4. A copy of the inofficial translation of the Austrian Data Protection Act was attached.*

---

* Available for consultation in the files of the secretariat.

## Croatia

[Original: English]
[4 September 1996]

1. The Government of the Republic of Croatia has, through its competent bodies, carefully considered the guidelines for the regulation of computerized personal data files adopted by the General Assembly in resolution 45/95 in order to implement its provisions at the national level both through legislation and practice.

2. At present, there is no existing comprehensive legal text concerning the regulation of computerized personal data files. Nevertheless, such regulation is included in separate legal texts concerning particular areas of public life where protection of personal data is needed, notably internal affairs, citizenship and personal status issues, medical care and, to a certain extent, the execution of penal sanctions. Moreover, certain questions of regulation of computerized personal data files are regulated by internal regulations of the respective government and public bodies dealing with the above-mentioned issues.

3. The process of drafting a comprehensive legal text on the regulation of personal data files is currently under way and is expected to enter the parliamentary procedure in the course of autumn 1996.

4. In the process of preparation of the draft of the said legal text, several international instruments have been taken as a standard for protection, notably the Council of Europe Convention on the Protection of Individuals Against the Unauthorized Use of Personal Data Files, the United Nations guidelines referred to above and the most recent European Union Directive on this matter of 1996. In addition, recently adopted national legislation of several European countries have also been taken into account in the drafting process.

5. Once adopted, this legal text will surely contribute to strengthening the protection and unifying standards of use of personal computerized data files.

## Estonia

[Original: English]
[10 September 1996]

The respective authorities of Estonia consider the United Nations guidelines for the regulation of computerized personal data files fully reasonable and applicable.

Germany

[Original: English]
[12 September 1996]

1. Pursuant to the Data Protection Directive 95/46 of the European Parliament and the Council of 24 October 1995, EU member States generally have to adapt their national data protection legislation. The enactment of the Directive provisions has to be effected by 23 October 1998. However, most of the requirements established by the Directive are already enshrined in the German data protection law. At present, the following developments are beginning to take place as regards some of the principles contained in the United Nations data protection directive in excess of the situation depicted in document E/CN.4/1990/72.

Principle 4

2. Data protection will be made more transparent for the citizen. This will be brought about by, among other things, extending the obligation to inform the data subject of the storage/communication of his data to the public sector, by introducing also in the private sector the general obligation to inform the data subject of the collection of his data, and by slightly enlarging the data subject's right of access.

Principle 9

3. In the course of adapting the data protection legislation to the EC Data Protection Directive a provision will have to be introduced which will make the communication of data to third countries contingent on the existence of an adequate data protection level in that country. Furthermore, a comprehensive list of exceptions to this principle must be introduced designed to prevent trade with third countries from being impaired. Furthermore, legal regulations are to be created, which keep data processors from moving to non-EU States with a lower data protection level, by making the national provisions adopted to enact the EC Directive apply also in these countries, if the means of processing, for instance terminals, questionnaires etc. are in the territory of an EC member State."

Libyan Arab Jamahiriya

[Original: Arabic]
[2 October 1996]

1. Having studied the draft guidelines for the regulation of computerized personal data files to which reference was made in General Assembly resolution 44/132 and which emphasize the need to respect the human rights and fundamental freedoms of individuals, the Socialist People's Libyan Arab Jamahiriya, while affirming its support for those principles in keeping with its consistent policy of defending the freedom and protecting the rights of human beings wherever they may be, and in accordance with its legislation based on the precepts of the Holy Qur'an which sanctify the human person as God's deputy on earth and, in particular, based on the Great Green Document on Human Rights, has embodied its convictions on the above-mentioned matter in

the Information Act No. 4 of 1990 concerning the national data and documentation system, article 6 of which deals with personal data in a manner that is fully consistent with the above-mentioned guidelines.

Article 6 of the Information Act

2. It is prohibited to use any means of coercion or deception to gather personal information or data within the framework of the National Information System. The person concerned has the right to view such information and data and to delete or rectify anything which, in his opinion, is at variance with the true state of affairs before it is documented.

3. The use of such data or information is confined to the purposes of economic and social studies. No third party, even if it is a public authority, is allowed access thereto and it is not permissible to disseminate them in a manner that indicates the identity of the persons concerned, nor can they be used for any other purpose or admitted as evidence or grounds for any legal proceedings in violation of the above stipulations.

4. It should be noted that this article of the Libyan Act embodies the following principles:

1. Lawfulness and fairness in the collection of personal data.

2. Verification of the reliability and accuracy of the personal data.

3. The purpose of the collection of the data.

4. Access by the persons concerned to the files containing their personal data.

5. Non-discrimination, for which the article makes implicit provision by prohibiting dissemination or use of the information for purposes other than those permitted by law in such a way as to indicate or reveal the identity of the persons concerned.

5. The other guidelines concerning the principles of security, supervision and sanctions are covered by articles 7, 8 and 9 of the Libyan Information Act.

6. On this basis, the Jamahiriya has adopted those principles, which it regards as the minimum guarantees that must be provided in order to safeguard basic human rights.

## Luxembourg

[Original: French]
[22 August 1996]

1. The modified Act of 31 March 1979 regulating the use of personal data in computer systems conforms 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, except as

regards principles 8 (supervision and sanctions) and 9 (transborder data flows), whose provisions are not expressly reproduced in our legislation.

2. Those principles will be incorporated by a new Luxembourg Act on the protection of individuals with regard to the processing of their personal data, which will transpose into national law the provisions of Directive 95/46/EC of the European Parliament and of the Council, of 24 October 1995, on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The transposition is due to take place three years from the adoption of the directive.

## Mauritius

[Original: English]
[10 September 1996]

The Government of Mauritius will introduce shortly an Information Technology (Miscellaneous Provisions) Bill, which among other things deals with offences in the field of data protection, data security and computer misuse.

## Mexico

[Original: Spanish]
[21 October 1996]

1. Principle of lawfulness and fairness. As regards this principle, the National Registry of Population and Personal Identification is governed by the General Population Act and its functions, as defined by article 87 of that Act, are to register Mexicans by means of the National Registry of Citizens, the National Registry of Minors and the Register of Mexicans Resident Abroad, and to register aliens through the Catalogue of Aliens Resident in the Mexican Republic.

2. At present, work is proceeding only on the creation of the Registry of Minors, for which information is obtained from the birth certificates submitted by civil registry offices throughout the Republic starting from 1982, as specified by article 89 of the General Population Act.

3. The civil registry offices are governed by the laws passed by the local congresses, which define how the respective entries are to be made in order to comply with the principle of legality and also determine the provisions necessary for observance of the principle of lawfulness and fairness.

4. Principle of accuracy. The National Registry of Population and Personal Identification has the obligation to check on the accuracy and relevance of the data recorded, by validating fields to avoid errors in data entry and by requiring certain fields to be defined to prevent the omission of important information.

5. Principle of purpose-specification. The above-mentioned Act complies with this principle since, although only the Registry of Minors is in

existence, the Act states in article 86 that the purpose of the National Registry of Population and Personal Identification is to register all persons making up the country's population using data enabling their identity to be certified or attested reliably. The aim of this is ultimately to issue the citizen's identity card, which will be the official document of identification, fully endorsing the data contained in it concerning the holder.

6. Since the birth certificate or naturalization paper, as a nationality certificate, is essential for personal registration, the laws governing the civil registry offices require them to be public, so that anyone can request an attestation from their records.

7. As for the information in the National Registry of Population and Personal Identification, however, it is considered that only the person concerned and the judicial authorities may have access to that information. In the case of the persons concerned, the Act provides for minors to be issued with an identification paper and adults with the citizen's identity card.

8. Regarding the conservation of personal data, this must be permanent, since even the death certificate has to be recorded. That brings us to another purpose of the registry, as stated in article 112 of the above Act, namely to provide the Federal Electoral Institute with the information it needs from the National Registry of Citizens in order to compile electoral instruments.

9. Principle of interested-person access. The second paragraph of article 36.1 of the Constitution of the United Mexican States specifies that the National Registry of Citizens and the issuance of the citizen's identity card are services in the public interest and, consequently, a responsibility for the State and for citizens.

10. The General Population Act provides for the issuance of the citizen's identity card, or of the identification paper for Mexicans under 18 years of age. In this connection, the persons concerned are allowed access to such information to avoid unlawful, invalid or inaccurate entries, although the Act itself does not provide the means for them to be corrected.

11. Principle of non-discrimination. The information obtained by the National Registry of Population and Personal Identification comes from the records of the civil registry office and the laws governing this institution categorically proscribe the recording of data which may give rise to unlawful or arbitrary discrimination, so that information not included in those records cannot possibly be entered into the database.

12. Power to make exceptions. Public use of the information contained in the database of the National Registry of Population and Personal Identification is provided for in article 112 of the General Population Act, which requires the Ministry of the Interior to provide the Federal Electoral Institute with the information it needs from the National Registry of Citizens to compile electoral instruments.

13. Principle of security. In order to protect files against natural hazards, accidental destruction and any of the other risks mentioned in paragraph 7 of the guidelines for the regulation of computerized personal data files, the National Registry of Population and Personal Identification makes backup copies of the information in its database and sends them to a safe storage facility outside its offices.

14. Supervision and sanctions. The General Population Act in article 113 sets out the sanctions which the authorities of the Ministry of the Interior, as the branch of government responsible for the database in the internal legal system, may apply to employees breaching the established rules in various ways, such as by supplying information on confidential matters without authorization, impeding the normal processing of files by fraud or gross negligence, interfering in the handling of legal matters or encouraging or advising on ways to avoid provisions and procedures, either themselves or through intermediaries.

15. Transborder data flows. Only the National Registry of Population and Personal Identification is to receive information from Mexicans established abroad. Such information will, however, be obtained through the Ministry of Foreign Affairs in accordance with article 96 of the General Population Act.

## Philippines

[Original: English]
[15 November 1996]

The Government of the Philippines submitted the following documents* provided by the Civil Service Commission (CSC) of the Philippines:

(i) Implementing Rules dated 21 April 1989 of Republic Act No. 6713 of 20 February 1989 entitled “Code of Conduct and Ethical Standards for Public Officials and Employees”;

(ii) CSC Resolution No. 92-1908 of 25 November 1992 entitled “Clarification on the Law of Transparency under the 1987 Constitution and R.A. 6713"; and

(iii) CSC Memorandum No. 73 series of 1993.

The information contained therein supplements the Philippine Government's report on its implementation of the guidelines submitted on 22 September 1994 (see E/CN.4/1995/75).

* Available for consultation in the Secretariat.

San Marino

[Original: Italian/English]
[5 and 11 September 1996]

1. As far as the computerized collection of confidential data is concerned, the legislation currently obtaining in the Republic of San Marino is constituted by Law N. 70 of 23 May 1995 (Reform of Law N. 27 of 1 March 1983, Regulating the Computerized Collection of Personal Data), and by Law N. 71 of 23 May 1995 ("Regulation on Statistical Data Collection and Public Competence in Data Processing"), the latter regarding more specifically data processing within the Public Administration.

2. Attempts to regulate the matter, however, had already been made previously. Notably Law N. 70 of 1995 repealed and totally replaced Law N. 27 of 1 March 1983 with the exception, however, of a series of Regency's Decrees which were passed to implement Law 27/83:

Decree N. 7 of 13 March 1984, "Establishment of a State Data Bank as provided for by Article 5 of Law N. 27 of 1 March 1983";

Decree N. 7 of 3 June 1986, "Integration to Decree N. 7 of 13 March 1984, Establishing a State Data Bank";

Decree N. 140 of 26 November 1987, "Procedures for the Establishment of Private Data Banks".

3. Article 20, paragraph II of Law 27/83 clearly states that these Decrees continue to be enacted, compatibly with the new regulation.

4. Law 70/95 plays a more crucial role with regard to the investigation that is being carried out. It introduced in the Sammarinese legal system a series of general principles safeguarding personal data files. After a careful examination, these principles were declared as perfectly in line with those affirmed by the Commission on Human Rights, setting a standard with which any national regulation should comply.

5. The Sammarinese legal system asserts the principles of legality and loyalty by clearly prohibiting in article 7, paragraph 1 of Law 70/95, the collection of personal and confidential data through fraudulent, illegal or unfair means.

6. Those in charge of the setting up and management of data banks are expressly required to abide by the principles of accuracy, relevance and completeness, as clearly implied by article 14 of Law 70/95, containing the obligation to rectify, update and integrate data ex officio whenever inaccurate or incomplete information is noted. Article 14 also envisages that any rectification, integration or updating be notified to the people concerned free of charge.

7. As regards the reasons leading to the setting up of a computerized filing system, the legislation obtaining does not define the specific aims that should be attained. The latter can rather be inferred from the procedure

that must be followed to create a data bank, which required the prior authorization of both the State Congress (the Government) and the Guarantor for the Safeguard of Confidential and Personal Data (art. 15). Therefore, any specific goal motivating the creation of a data bank is ultimately stated by the above-mentioned bodies jointly. Moreover, any person contacted in relation to the collection of personal data destined to be computerized must be duly informed of the objectives pursued (art. 8). Admittedly, this principle requires further specification.

8. Conversely, the Sammarinese legal system safeguards the right of access to files and records and confidential data very effectively, in that any individual is entitled both to inquire whether his or her personal data have been collected or processed (art. 10) - and obtain a copy accordingly (art. 11) - and to require that inaccurate, outdated, incomplete or ambiguous data, or data whose collection, processing, transmission or preservation is forbidden, be rectified, integrated, clarified, updated or cancelled (art. 12).

9. In any case, should doubts arise on the veracity and conformity of collected and processed data, written statements can be addressed to the Guarantor, who is to provide an answer within 60 days from reception, after having considered whether an administrative investigation or intervention by the Magistracy is necessary (art. 13); a petition can be made accordingly.

10. Law 70/95 fully sanctions the principle of non-discrimination, which allows the gathering of special information only provided that the people concerned consent to it, since that (for example, information regarding political, trade union, or religious ideas or activities) could lead to illegal or arbitrary discrimination. The gathering of extremely personal information is prohibited in any case (art. 7).

11. The principle of security, envisaging appropriate measures to avert potential destruction of files/records and prevent unauthorized access, is expressed in general terms by article 4, paragraph IV. The article provides that data bank staff should observe professional secrecy rigorously, and envisages precautionary measures to prevent information from being biased. counterfeited or disclosed to unauthorized people.

12. With specific reference to controls on the effective observance of the above-mentioned principles, this function is attributed to the Guarantor for the Safeguard of Confidential and Personal Data, who is the authority competent to examine any claim or petition relating to the application of the above-mentioned law and pass judgement whenever the confidentiality of personal data is violated. A higher court, however, be it ordinary or administrative, can always be appealed to. Other functions to be accomplished by the Guarantor are also determined by the law (arts. 15 and 16). The way in which this body has been conceived fully meets the need to guarantee the impartiality and independence of the staff dealing with the computerization of confidential data. The Guarantor's tasks are accomplished by a judge of the Administrative Court.

13. In order to ensure maximum protection of confidential data and more effective enforcement of relevant laws, the infringement of certain norms is punished by means of administrative sanctions or penalties (arts. 17 and 18).

14. As regards confidential data on Sammarinese individuals being transferred outside the borders of the Republic, the release of information is conditioned on the prior and motivated authorization of the Guarantor, who will have to verify whether the country to which confidential information is being transmitted ensures the same level of protection of personal data as that established in Sammarinese legislation.

15. Law 70/95 has a wide and generalized range of application, since it is applicable, with no distinction, to any computerized filing system or data bank, both private and public, owned by either a physical or legal person (art. 1).

16. In conclusion, the legislation obtaining in the Republic of San Marino as regards the protection of confidential and personal data is substantially in line with the principles affirmed by the Commission on Human Rights.

## Sweden

[Original: English]
[26 August 1996]

1. Sweden submitted a report on this subject in August 1994 (see E/CN.4/1995/75) which is, with some amendments, still valid. As mentioned in that report, the Government presented a bill to Parliament on 14 April 1994 with certain amendments to the Data Act of 1973. These amendments entered into force on 1 January 1995. The report of 1994 contains a description of these amendments.

2. There is however one change in the amendments compared to what is said in that report: not all appeals against the Data Protection Agency's decisions are supposed to be handled by a court of justice. If the complainant is a public authority under the Government, the appeal is still handled by the Government.

3. At present, the main legislative question regarding data protection issues concerns the new directive of the European Union on the protection of individuals with regard to the processing of personal data and the free movement of such data (Directive 95/46/EC). The member States are given a period of three years during which they can transpose the Directive into national law, starting from the date of adoption. The Directive was adopted on 24 October 1995.

4. The Government has set up a special parliamentary commission to draft totally new data protection legislation within the framework of the EU Directive. The instructions from the Government to the commission include that the law shall apply to personal data irrespective of the type of technique used. The commission will finish its work before the end of March 1997.

United Kingdom of Great Britain and Northern Ireland

[Original: English]
[30 September 1996]

1. 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 or her, 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.

2. The key features are as follows:

(i) 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 (for example, the Electoral Register); or where data is held for national security purposes (as determined by government ministers).

(ii) 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.

(iii) 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 for the registered purpose; and surrounded by proper security.

(iv) The Registrar may serve three types of notice to enforce compliance with the principles: an enforcement notice specifying action to take, a deregistration 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.

(v) 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 him or her (except, for example, where such subject access would be likely to prejudice the prevention or detection of crime). He or she may complain to the Registrar or apply to the courts for an order if access is not given within 40 days.

(vi) If a data subject considers there has been a breach of one of the principles or any provision of the Act he or she 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.

(vii) 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” (for example, disclosure required by law or made with the data subject's consent).

(viii) The Registrar reports directly to Parliament. She holds the Register of data users and computer bureaux and 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. She considers complaints about breaches of the principles or Act and, where appropriate, prosecutes or serves notices.

(ix) 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.

3. On 3 February 1995 the Act was amended to make it an offence for a person to procure the disclosure of personal information, if that person knows or has reasonable grounds to believe that the disclosure in question constitutes a breach of the Data Protection Act; and to make it a separate offence for that person to sell or offer for sale the data which he or she has so procured. This provision strengthens the 1984 Act's protection of the security of personal data. It was introduced in response to concern about the activities of firms of inquiry agents which were offering confidential personal information (including financial information) for sale.

## Uruguay

[Original: Spanish]
[11 June 1996]

1. Uruguay has not thus far enacted any special penal laws dealing with "computer crime". However, national doctrine considers that the guidelines which must govern the use of computerized personal files are recognized and protected by the legislation currently in force.

2. As regards Uruguayan law, reference should be made first to the Constitution, and in particular:

> Article 7, which establishes that the inhabitants of the Republic are entitled to protection, inter alia, of their honour, labour and property. No one may be deprived of those rights except in conformity with such laws as are enacted for the general welfare;
>
> Article 19, which provides that no inhabitant shall be obliged to do what the law does not require, or be deprived of what it does not prohibit;
>
> Article 32, which establishes that ownership is an inviolable right, but is subject to the provisions of laws relating to the general welfare. No one may be deprived of his property rights except in the cases of public necessity or utility defined by law and with fair compensation in advance from the National Treasury;
>
> Article 33, which stipulates that intellectual property and the rights of authors and inventors shall be recognized and protected by law;
>
> Article 36, which establishes that every person may engage in labour, industry, commerce, a profession or any other lawful activity, save for the limitations imposed by law for the general welfare.

3. In addition to these specific norms, article 72 reads as follows:

> "The enumeration of rights, duties and guarantees made in the Constitution does not exclude others which are inherent to the human person or derive from the republican form of government."

4. Furthermore, article 332 states that:

> "The precepts of the present Constitution recognizing rights for individuals and conferring powers and imposing duties on the public authorities shall not cease to be applicable for lack of appropriate regulations, which shall be supplied having regard to analogous legal tenets, to general principles of law and generally accepted doctrines."

5. The above norms provide a sound conceptual framework for the protection of the rights which are to be safeguarded. [1]

6. It should at the same time be pointed out that the lack of concrete juridical norms for dealing with the particular issue of databases could be remedied by the action of amparo provided for by Act No. 16,011 of 19 December 1988, article 1 of which states that:

> "Any natural person or juridical person, whether public or private, shall be able to bring an action of amparo against any act or omission of a public or semi-public authority or individual which in that person's opinion actually or potentially impairs, restricts, alters or threatens, with manifest unlawfulness, any of his or her rights or freedoms as expressly or implicitly recognized by the Constitution (art. 72), except in cases where the remedy of habeas corpus is applicable." [2]

7. Under this Act, the compiler of a database, for example, might bring amparo proceedings against anyone impairing, altering or threatening the right enshrined in article 33 of the Constitution - in other words, his intellectual property. Similarly, the investor might take such action to protect his property rights (arts. 7, 32 and 36 of the Constitution). The average man, too, could protect his right to privacy - recognized implicitly by article 72 of the Constitution - by causing the cessation of the act or omission of the authorities or individuals which in his opinion impairs, restricts, alters or threatens the disclosure, misuse or other such possible application of his personal data. [3]

8. Cases of fraudulent inclusion of inaccurate information about persons in files may be considered in the light of article 240 of the Uruguayan Penal Code, which reads:

> "Anyone who makes a false private document or alters a true one shall, upon making use of it, be punished by a term of twelve months' ordinary imprisonment to five years' rigorous imprisonment."

9. In cases where false representation is actively practised by a public official, the applicable provision may be article 238 of the Penal Code, which reads:

> "A public official who, in the exercise of his functions, attests to the occurrence of imaginary facts, or attests to real facts but alters the circumstances, or omits or modifies statements made with that intention or suppresses such statements, shall be punished by two to eight years' rigorous imprisonment."

10. Concerning due respect for the principle of purpose-specification, the disclosure of personal data without valid reason is penalized by articles 301 and 302 of the Penal Code, which stipulate as follows:

> "Article 301. Anyone who without just cause reveals the contents of the documents mentioned in the preceding article (whether public or private), which have been brought to his knowledge by the means defined therein or by other unlawful means, shall be punished by a term of three months' ordinary imprisonment to three years' rigorous imprisonment."

"Article 302. Anyone who without just cause reveals secrets brought to his knowledge by virtue of his profession, occupation or mission shall, where such action causes injury, be punished by a fine of 100 to 2,000 pesos."

Notes

1.Mario Barreto Gugelheim, "Protección jurídica de la base de datos", in La Justicia Uruguaya, vol. 108, 1994, pp. 41-50.

2.N. Bergstein, "Derecho penal e informática", in La Justicia Uruguaya, vol. 111, 1995, pp. 43 et seq.

3.Mario Barreto Gugelheim, "Protección jurídica de la base de datos", in La Justicia Uruguaya, vol. 108, 1994, pp. 41-50.

---