UNITED
NATIONS

A

General Assembly

Distr.
GENERAL

A/44/606/Add.1
15 December 1989

ORIGINAL: ENGLISH

Forty-fourth session
Agenda item 107

HUMAN RIGHTS AND SCIENTIFIC AND TECHNOLOGICAL DEVELOPMENTS

Guidelines for the regulation of computerized personal data files

Report of the Secretary-General

Reply received from Austria

1. Austria welcomes the guidlines for the regulation of computerized personal data files. The "humanitarian clause" contained in principle 11 has been noted with particular interest and satisfaction. A clause to that effect is fully compatible with Austrian legislation on the protection of personal data.

2. In Austria's view, the right to obtain information concerning oneself contained in principle 4 should be extended to knowledge about which data have been passed on and to whom.

3. Finally, legislation protecting files of legal persons exists not only in Denmark, Luxembourg and Norway but also in Austria (p. 7, para. 29).

Reply received from Canada

Guidelines on the use of computerized personal files adopted by the Commission on Human Rights

1. The Canadian Government commented in 1986 on the first version of the above-captioned guidelines. The following remarks compare the current version of the Guidelines to the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data adopted by the Organisation for Economic Co-operation and Development (OECD), 23 September 1980, and to which Canada adhered on 29 June 1984. The following comments also take into account the provisions of the Canadian Privacy Act.

Principle 1. Lawfulness and fairness

2. As stated in the 1986 comments of the Government of Canada:

> "Pursuant to section 4 of the Privacy Act, personal information shall only be collected by government institutions if it relates directly to operating programs or activities of those institutions. Section 5 sets out the principles of collection including information which must be supplied to the individual at the time of collection; exceptions are provided at subsection 5 (3) of the Privacy Act where application of the principles might either result in the collection of inaccurate information or defeat the purpose or prejudice the use for which information is collected."

3. Article 7 of the OECD Guidelines states that "data should be obtained by lawful and fair means", that there should be limits to such collection and that the "knowledge or consent of the data subject" should be obtained "where appropriate".

Principle 2. Accuracy

4. Section 6 (2) of the Privacy Act specifies that personal information used for an administrative purpose by a federal institution is "as accurate, up-to-date and complete as possible". The United Nations draft guidelines have removed the reference to completeness on the grounds that "personal information can never in fact be complete" (see E/CN.4/Sub.2/1988/22, para. 14).

5. As is the case with the Privacy Act, the OECD Guidelines stipulate that "personal data ... should be accurate, complete and kept up-to-date", thus incorporating the concept of "complete information" which has been removed from the United Nations draft guidelines on the grounds that personal information can never be "complete".

6. The United Nations draft guidelines suggest a regular update of personal information files. The Government of Canada respectfully submits that such an update, when a file is not being used, is unnecessary and constitutes an invasion of privacy.

Principle 3. Purpose-specification

7. Section 5 of the Privacy Act enunciates the general principle in terms of purpose-specification, stating that information should, wherever possible, be collected from the individual to whom it relates and its purpose should be specified at the time of collection. However, direct collection or purpose-specification do not apply when they "might result in the collection of inaccurate information; or defeat the purpose or prejudice the use for which information is collected", as stipulated in subsection 5 (3) of the Privacy Act.

8. Paragraph 8 (2) (a) of the Privacy Act enables the disclosure of personal information for a use compatible to the use for which the information was originally compiled.

9. Furthermore, the Privacy Act permits information to be disclosed for purposes not incompatible with the Act as set out in subsection 8 (2).

10. In addition, an index stating the purposes and uses consistent with these purposes of all personal information banks must be published annually pursuant to subparagraph 11 (1) (a) (iv) of the Privacy Act.

11. With respect to the fact that the United Nations guidelines specify that data should remain relevant and adequate (subsection 6 (2) Privacy Act), that it not be used or disclosed improperly (sects. 7 and 8 Privacy Act) and that the retention of personal information not be unreasonable (subsections 6 (1) and (3) Privacy Act), it should be noted that subsection 37 (1) of the Privacy Act vests the Privacy Commissioner with the power to conduct investigations to ensure compliance with sections 4 to 8 which constitute the Code of Fair Information Practices.

12. Article 9 of the OECD Guidelines deals with purpose specification. The proposed United Nations guidelines state that the purpose should be "legitimate", a concept which is not expressly embodied by the OECD Guidelines. The exceptions provided for in article 10 of the OECD Guidelines dealing with the use limitation principle are not a part of the purpose specification principle of the proposed United Nations guidelines.

Principle 4. Interested-person access

13. The right to be given access to personal information under subsection 12 (1) of the Privacy Act has been extended by Order in Council (SOR/89-206) (copy attached) to include all individuals "present in Canada" i.e. who are physically situated in the country. Paragraph 12 (2) (a) of the Privacy Act enables an individual to request corrections of personal information while paragraph 12 (2) (b) requires that a notation be attached to the information when a correction is requested but not made. In addition, the Privacy Act, at paragraph 29 (1) (c), empowers the Privacy Commissioner to investigate complaints from individuals alleging that such corrections are being refused without justification.

14. The OECD Guidelines' article 13 provides individuals with the right to obtain information or confirmation of whether or not there is information relating to them. It also provides the right to have information communicated and to be given reasons if a request for information is denied. Finally, it foresees the right to challenge data and to have the data corrected if the challenge is successful. The OECD Guidelines do not provide for any other remedy nor do they specify that the cost of correcting data should be borne by the person responsible for the file, as is the case with the proposed United Nations guidelines.

15. The Privacy Act does not go as far as the OECD Guidelines or the proposed United Nations guidelines in terms of giving access to the interested person.

Principle 5. Non-discrimination

16. Section 4 of the Privacy Act restricts the collection of personal information to information which "relates directly to an operating program or activity" of a government institution.

17. The Charter of Rights may serve as a basis to challenge the collection of discriminatory data.

18. The OECD Guidelines do not deal expressly with the issue of discrimination, stating simply "personal data should be relevant to the purposes for which they are to be used" and that the "purposes for which personal data are collected should be specified not later than at the time of data collection" (arts. 8 and 9).

Principle 6. Power to make exceptions

19. Section 2 of the Access to Information Act stipulates that exemptions to the right of access are "limited and specific". These exemptions are contained in sections 18 to 28 of the Privacy Act. In addition, subsection 5 (3) of the Privacy Act allows for exemptions to purpose specification when compliance with subsections (1) and (2) might "result in the collection of inaccurate information" or "defeat the purpose or prejudice the use for which information is collected".

20. As stated in the 1986 comments from the Canadian Government, we would rather not limit ourselves to only those cases identified in the United Nations guidelines and we respectfully suggest that a slight change in the wording might accommodate our preference: "Departures ... may be admitted in certain cases, such as ...". Considering the range of exemptions foreseen in the Act, such as international relations, federal-provincial relations, solicitor-client privilege, it may well be that some of those exemptions are not covered by those enumerated in the proposed United Nations guidelines.

21. Article 10 of the OECD Guidelines states that data should not be disclosed without the consent of the data subject or without the authority of the law. Furthermore, section 4 of the OECD Guidelines stipulates that "exceptions to the Principles ... including those relating to national sovereignty, national security and public policy ("ordre public"), should be as few as possible and made known to the public".

Principle 7. Security

22. Sections 6, 7 and 8 of the Privacy Act create an obligation for government institutions to ensure the essential security of personal information against unauthorized access, destruction use, alteration or disclosure.

23. This protection is enhanced by the Government Security Policy issued by Treasury Board, circular 1986-26 on 18 June 1986. This policy heightens the protections afforded by the Privacy Act by setting down requirements for the physical security of information.

24. The principle of security is embodied by article 11 of the OECD Guidelines.

Principle 8. Supervision and penalties

25. The Privacy Commissioner's office which is created in virtue of sections 53 to 67 of the Privacy Act ensures the government institutions' compliance with the Code of Fair Information Practices by way of investigations concerning personal information. The Privacy Commissioner reports to Parliament.

26. Section 126 of the Criminal Code states that "everyone who (...) contravenes on Act of Parliament (...) is, unless a punishment is expressly provided by law, guilty of an indictable offence (iii)".

27. Article 14 of the OECD Guidelines stipulates that a "data controller should be accountable for complying with measures which give effect to the principles" of the Guidelines.

Principle 9. Transborder data flows

28. The Privacy Act deals with information collected by federal government institutions. It foresees situations where information may be exchanged with other Governments (subsection 8 (2)) but does not deal with transborder data flows any further.

29. Articles 15 to 18 of the OECD Guidelines deal with transborder flows of information, stipulating that all steps should be taken to ensure that information flows are uninterrupted and secure and that member countries should avoid developing laws and policies that would create obstacles to transborder flows of information.

30. The Canadian Government having adhered to the OECD Guidelines, promotes the voluntary compliance of private sector enterprises under its jurisdiction with the Guidelines to facilitate transborder data flows.

Principle 10. Field of application

31. As stated in the 1986 comments of the Canadian Government:

> "The Privacy Act applies to all personal information under the control of government institutions to which it applies, whether it be computerized or recorded in other forms including manual data systems".

32. The scope of the OECD Guidelines is dealt with in articles 2 and 3. The Guidelines apply to both automated and non-automated fields.

Principle 11. Application of the guidelines to personal data files kept by governmental international organizations

33. Article 3 of the OECD Guidelines deals with the scope of the Guidelines while article 16 of the said Guidelines stipulates that flows of personal data are uninterrupted.
