UNITED NATIONS

E

Economic and Social Council

Distr.
GENERAL

CES/2003/10
7 April 2003

ORIGINAL: ENGLISH

STATISTICAL COMMISSION and ECONOMIC COMMISSION FOR EUROPE

CONFERENCE OF EUROPEAN STATISTICIANS

Fifty-first plenary session
(Geneva, 10-12 June 2003)

LEGAL ASPECTS – LEGISLATION IN THE NORDIC COUNTRIES

Paper submitted by Statistics Sweden[1]

I. INTRODUCTION

1. This paper presents some of the legal issues concerning access to microdata and describes the legislation in the Nordic countries. The paper is based on the Nordic Statistical Agencies report "Access to microdata in the Nordic countries".

2. National Statistics Institutions (NSIs) are dependent on the confidence of the respondents, and they are required to respect confidentiality and protect individual's integrity. The willingness of respondents to provide data is dependent on the ability of statistics offices to guarantee respondents anonymity.

3. Confidentiality protection of individual and business data is one of the main principles of official statistics. The individual is entitled to be protected by society against unacceptable intrusion of personal integrity. At the same time the need of the individual for protection must be balanced against legitimate needs of using information connected to people, for example, for purposes of statistics and research. Microdata collected for statistical purposes is of vital interest for researchers. In recent years the demands to make statistical microdata available for research purposes have increased. Researchers also ask for more and more detailed data. A considerable amount of balancing is necessary when formulating legislation to protect personal integrity as regards personal data. Furthermore, legislation

[1] Prepared by Birgitta Pettersson.

must not unnecessarily restrict the use of new technology, which brings with it not only risks but also advantages.

4. The protection measures applied to confidential data obtained for statistical purposes are based on several legal acts and directions. It is important that the regulation concerning statistics and confidentiality is clear and well suited to its purpose. Clear rules are needed to create confidence, especially with the respondents. The legislation concerning confidentiality and protection of individual's integrity is of importance for the possibility of the NSI to provide access to microdata. The legislation provides the limits for release of data for e.g. research purposes, and underpins and constitutes administrative and technical safeguards for legal founding. Specific legislation of importance in the Nordic countries is the Statistics Act and the Data Protection Acts. To this specific legislation, the current EU legislation with respect to statistical confidentiality should also be added.

II. GENERAL RULES

5. The use of statistical information is often regulated by legislation or in a code of practice. In the Nordic countries there are specific Statistics Acts regulating the use of statistical information. According to these acts, data collected for statistical purposes, in accordance with any prescribed obligation to provide information or which is given voluntarily, may in principle only be used for the production of statistics. There are exceptions that allow access to data for research purposes and public planning. However, a condition for the use for research is that there is no incompatibility between the purpose of such processing and the purpose for which the data was collected. The processing of data, which includes release of data, must also be in accordance with the regulation concerning protection of individual integrity.

6. The general personal data protection acts in the Nordic countries, (the Personal Data Acts[2]) also apply to the production of statistics and the release of microdata. The Acts are based on the 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 Acts contain rules about the fundamental requirements concerning the processing of personal data. The Personal Data Acts are similar in the Nordic countries and apply to all forms of processing of personal data, including registration, storing, disclosure, merging, changes, deletion, etc.

7. According to the Personal Data Acts, data must be:

- Processed fairly and lawfully.
- Collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. However, further processing of data for historical, statistical or scientific purposes is not considered as incompatible.
- Adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

[2] In Denmark - the Act on Processing of Personal Data, Act No. 429 of 31 May 2000, Finland - The Personal Data Act 523/1999, Island - Act on the Protection of Individuals with regard to the Processing of Personal Data 77/2000, Norway –the Personal Data Act (2000), Sweden - the Personal Data Act (1998:204).

- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, with regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
- Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed. Personal data can be stored for longer periods for historical, statistical or scientific use.

8. If data about a person is collected from the person him/herself, the controller of personal data shall in conjunction therewith voluntarily provide the person in question with information about the processing of the data.

9. Very stringent rules apply to the processing of sensitive personal data. Sensitive data is personal data that discloses race or ethnic origin, political opinions, religious or philosophical convictions, membership of trade unions and personal data relating to health or sexual life. The main principle is that such data may be processed only with the consent of the person in question. However, sensitive data may be processed for research and statistical purposes without consent, provided the processing is necessary and provided the public interest in the project clearly exceeds the risk of improper violation of personal integrity.

10. Furthermore in Denmark, Norway and Sweden a scientific project involving processing of sensitive personal data without consent is subject to notification to and approval by the Data Protection Agency before such processing can commence. This applies to all surveys, whether conducted by a public administration, individuals or enterprises. (In Sweden the approval of the National Data Protection Agency is not necessary if a research committee has approved the processing.) If the Data Protection Agency approves the processing, personal data may be released and used in research projects unless otherwise provided by the rules on confidentiality. This means that NSIs may take other issues into consideration even if the Data Protection Agency (or in Sweden a research committee) has approved the processing of data. The Data Protection Agency only considers whether the processing is in accordance with the Personal Data Acts. The NSIs must also consider whether data can be released without disclosing individual information.

III. CONFIDENTIALITY

11. Data, even anonymous data obtained for statistical purposes are confidential. The statistical data are confidential irrespective of source. Also data taken from public administrative sources are confidential while in the possession of the NSI. According to legislation in the Nordic countries, it is prohibited to disclose confidential data to unauthorized people. In Finland and Norway the provisions for confidentiality are regulated in the Statistics Acts. In Sweden, confidentiality of data shall be stated in a special statute, the Secrecy Act. The Secrecy Act contains provisions on what is to be kept confidential in state and municipal activities. Confidentiality in the Secrecy Act is usually expressed to apply in relation to certain matters, for certain operations and regarding certain public authorities. Confidentiality does not attach to the information released to another authority unless this is provided in the Secrecy Act.

12. According to the main principle in the Nordic countries, confidential data may be released to a third party only for the purpose of statistical surveys and research. Under the main principle, access may be granted in forms which do not allow direct or indirect identification of individuals or of other data subjects like enterprises. In practice the Nordic NSIs only provide access to anonymous data or microdata without name, address and identification number.

13. There is often no legal definition in national legislation that aims at whether an individual or enterprise is identifiable. However, the definition in the Council Regulation (EC) No 322/97 of 17 February 1997 on Community Statistics, Article 13 states: To determine whether a statistical unit is identifiable, account shall be taken of all the means that might reasonably be used by a third party to identify the said statistical unit.

14. The avoidance of indirect identification is difficult, especially when the data set includes a lot of detailed information that for example may have skewed distribution in statistics. This is the case in the so-called 'linked employer-employee data'. Disclosure of data is also a problem in small area statistics or statistics concerning business data where one entity is the sole producer.

15. The obligation of confidentiality will also – according to the law or by imposition of a duty of non-disclosure – apply to the recipient of the data. The NSI may also impose a restriction limiting the researchers right to re-communicate or use the information. Breach of confidentiality restrictions is punishable. In Sweden however, it is not possible to impose restrictions when data are released to other authorities. It is therefore important for Statistics Sweden to also take into consideration if data will be confidential according to the Swedish Secrecy Act by the authority receiving data. If not, anyone who so desires can have access to the data because of the authorities' obligation under Chapter 2 of the Freedom of the Press Act to provide access to data that are not confidential.

16. All exceptions from this principle of public access to official information must be stated explicitly in the Swedish Secrecy Act. The Secrecy Act does not contain any general rule concerning the transfer of confidentiality between public authorities. As a rule, that authority having its own confidentiality rule applicable to the information satisfies the need for confidentiality by the recipient authority. However, there are rules providing that secrecy accompanies information to another authority in special situations. One of these rules states that if an authority receives data for research purposes from another authority where the data is confidential, the confidentiality will also apply within the receiving authority. In practice this means that in most cases there is not any problem with providing access to microdata to researchers working at authorities, e.g. universities. However, there are no such rules concerning release of data for statistical purposes or public planning.

17. In addition to laws and regulations on data confidentiality, all the Nordic countries follow some kind of screening procedure requiring written confirmation that the researcher has signed a general confidentiality statement. Legal contracts are made that include various limitations to the access to microdata by specifying the people, projects, variables and periods during which data can be used in

the research. However, as previously mentioned, Sweden does not impose restrictions when data are released to another authority.

18. In practice, the Nordic NSIs will provide access to statistical microdata only for a specific research purpose. In principle, access to microdata is provided only to an authority, officially approved institution or individual "bona fide researcher".

IV. MAKING MICRODATA AVAILABLE

19. The legislation in the Nordic countries does not contain any rule that restricts the way of releasing microdata. As long as the general demands in the legislation are fulfilled, the NSI can chose to use a method. How access to confidential data is provided in practice can be divided into a few categories: Off-site access, on-site access, off-line access and on-line access.

20. In Norway and Sweden, data sets on individuals or enterprises are delivered to researchers that are working outside the statistical office. This approach is also widely used in Finland, but mostly with personal data sets. Business data sets, however, are infrequently delivered to external users, and only after very careful data inspection and protection that involves removing large firms and adding random noise to variables.

21. Statistics Denmark has another practice. Since its overriding principle is not to release data outside Statistics Denmark, they have set up a scheme with an on-site arrangement for external researchers at Statistics Denmark. Under this scheme, researchers can get access to register data that do not have identifying variables or are anonymous from a workstation at the premises of Statistics Denmark. Statistics Denmark also provides the user access to microdata from a special computer at Statistics Denmark, and the user has the possibility to manage this computer from his own office over an encrypted Internet communication. However, access is not granted for all datasets; particularly sensitive data are excluded from the scheme and data on enterprises are assessed carefully to avoid any problems of confidentiality.

V. RELEASE OF MICRODATA TO RESEARCHERS IN OTHER COUNTRIES

22. According to Directive 95/46/EC, Member States are required to provide that the transfer of personal data to a third country (a country outside the EU and EEA) may take place only if the third country in question ensures an adequate level of protection and the Member State laws implementing other provisions of the Directive are respected prior to the transfer. However, the Commission may find that a third country ensures an adequate level of protection. In that case personal data may be transferred from the Member States without additional guarantees being necessary. According to the Directive, the level of data protection should be assessed in the light of all circumstances surrounding a data transfer operation or a set of data transfer operations and in respect of given conditions. The Working Party on Protection of Individuals with regard to the Processing of Personal Data established under that Directive has issued guidance on the making of such assessments.

23. Switzerland[3], Hungary[4] and the US 'safe harbour' arrangement have been recognized as providing adequate protection. In order for US organisations to comply with the Directive, the US Department of Commerce in consultation with the European Commission developed a safe harbour framework. The EU approved the safe harbour principle in July of 2000[5]. Certifying to the safe harbour will assure that EU organisations know that an enterprise provides "adequate" privacy protection, as defined by the Directive. Safe harbour does not cover all organisations in the US.

24. The European Commission[6] has also recognized that the Canadian Personal Information Protection and Electronic Documents Act provides adequate protection for certain personal data transferred from the EU to Canada. However, the Canadian Act and the Commission Decision do not cover personal data held by public bodies, both at federal and provincial level, or personal data held by private organisations and used for non-commercial purposes, such as data handled by charities or collected in the context of an employment relationship.

25. For transfers of data to recipients in organisations not covered by the above-mentioned decisions and other countries, such recipients in the EU will have to enact additional safeguards, such as the standard contractual clauses adopted by the Commission in June 2001[7], before exporting the data.

26. In the Nordic countries, the same regulation concerning data confidentiality as for release of data outside the Statistics agencies is in principle also valid also when data is delivered to other countries. However there are some restrictions. The Personal Data Acts in the Nordic countries contain similar rules as the Directive that restricts release of data to a third country. According to the Personal Data Acts it is in principle forbidden to transfer personal data that is being processed to a third country unless the third country in question ensures an adequate level of protection.

27. In Sweden the Secrecy Act is also of relevance. According to the Act, release of confidential data to an authority or an international organisation outside Sweden is not allowed unless 1) it is released in accordance with special provisions in legislation, or 2) the data in a corresponding case might be given to a Swedish authority and the authority holding the data deems it evidently compatible with Swedish interest that the information is released.

---

[3] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland.
[4] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Hungary.

[5] Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce.
[6] Commission Decision of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act.
[7] Commission Decision (2001/497/EC) providing standard contractual clauses for the transfer of personal data to third countries.

28. The EU regulation includes special provisions that make it possible to release microdata to Eurostat. There are no other special provisions concerning statistical microdata. In Sweden release of microdata to an authority in other countries for research is therefore possible only if it is compatible with Swedish interest that the data is released. Microdata may be released to private researchers in other countries if it is clear that the information can be released without the person whom the information concerns suffering loss or being otherwise harmed. In practice Statistics Sweden is restrictive with release of microdata to researchers in other countries.

Statistics Norway only release anonymous microdata to researchers outside Norway and the researcher must fulfil the other conditions for release of data.

29. In Finland the same regulations concerning data confidentiality are valid as for the release of data outside Statistics Finland. The only exception is that the delivery of data outside Finland requires the approval of the Director General. However, before the Director General submits an application for the final decision, it needs to be addressed by the Data Protection Board. An applicant must provide the Board with a description on how the confidentiality of the data will be ensured outside Finland.

30. Denmark and Iceland do not provide access to microdata to researchers in other countries.

31. The release of information to Eurostat is regulated in the EU regulations on statistics. Member states are in principle bound by these regulations to release microdata for community statistics.

REFERENCES

Access to Microdata in the Nordic Countries (2003). Statistics Sweden.