

**STATISTICAL COMMISSION and
ECONOMIC COMMISSION FOR EUROPE**

**COMMISSION OF THE
EUROPEAN COMMUNITIES**

CONFERENCE OF EUROPEAN STATISTICIANS

EUROSTAT

**Joint ECE/Eurostat Work Session on
Statistical Data Confidentiality**
(Thessaloniki, Greece, 8-10 March 1999)

Working Paper No. 19 (Summary)
English only

Topic (iii) - Administration and policy of statistical data confidentiality

**DATA PROTECTION IN PRACTICE - ORGANIZATIONAL SOLUTIONS
AND PROTECTION MEASURES**

Submitted by Statistics Finland¹

Contributed paper

Summary

Basis of data protection

1. The Protection of confidential statistical data in Finland is based on several legal acts and instructions. The Statistics Act defines the general principles of data protection and access to confidential data. The Personal Data Act based on the EU's Data Protection Directive regulates processing of personal data. The Act on the Publicity of the Function of the Authorities provides that the authorities have to follow good data administration practice which also includes data protection. The need for a special act on data security is at present under discussion. The Government has given instructions and recommendations on data security for all state authorities. Statistics Finland has confirmed very detailed internal instructions on data security and access to confidential data. Statistics Finland also has an Ethical Guide for the whole personnel, which has proved to be a very effective instrument for understanding and internalising the principles of statistical confidentiality.

Organizational solutions

2. It is a part of the principle of impartiality that only statistical authorities have decision-making power on the right to use confidential statistical data. At Statistics Finland the decision-making system is decentralised. The Directors of Units grant access to individual data both to the personnel and to outside researches. They are also responsible for the implementation of data security instructions in their own units. Apart from the instructions, the decentralised system requires expert support in order to guarantee the uniformity of decisions made in different units. For support in decision-making, Statistics Finland has an expert body on access to confidential data and ethical questions, another expert body on data security, legal advisers and experts on data security. The centralised supervision of the whole data protection system belongs to the Director General, expert bodies and the internal auditor.

¹ Prepared by Riitta Harala and Anna-Leena Reinikainen.

Data protection principles

3. The practical basis for the protection of statistical data in Statistics Finland is a data protection classification. Its purpose is to classify statistical data material according to their confidentiality (sensitivity) into different groups. The main principle of the classification is the sensitivity of data from the point of view of personal integrity, the integrity of business enterprises or the safety of the country. The most important criteria are what the disclosure or misuse of data might cause to the interests to be protected.

4. The data protection classification forms the basis for deciding or regulating what kinds of protection measures each data material requires. The basic principle in data protection is that confidential micro data with identification data should not be released outside the statistical office unless it is regulated by law in exceptional cases.

Data protection classification

5. The data protection classes are as follows:

- Data material with highly confidential data, data protection class 3.
- Data material with very confidential data, data protection class 2.
- Data material with confidential data, data protection class 1.
- Public data material

6. Highly sensitive data equipped with identification data and regulated by the Personal Data Act² belong to the data protection class 3. This class also includes data files containing data which might endanger the safety of the country. In addition to these, extensive material containing several variables (for example census files) can be classified under this category. Material in the data protection class 3 or part of it must not under any circumstances fall into the hands of outsiders if it is not regulated separately by law in exceptional cases.

7. The data protection class 2 includes data material which does not contain highly sensitive data, but in which units (persons, enterprises, etc.) are identifiable and which cannot be released outside the statistical office. The majority of the micro data files of Statistics Finland belong to this class. Highly sensitive data from which the identification data are removed can also be classified under this category.

8. The data protection class 1 comprises data which are limitedly public. These data can be released outside the statistical office, but the use is limited. The limitations concern, for example, the purpose of the use of the data material. The material is compiled of data belonging to the data protection classes defined above. The data are made unidentifiable for example by aggregating or removing variables which would make it possible to identify units. It should be noted that removing identification data is not often enough to prevent identification.

²

1) racial or ethnic origin
 2) social, political or religious convictions of persons
 3) a criminal act, punishment or other sanction for an offence
 4) the state of health, illness or disability of person or treatment or other comparable measures to which he has
 5) the sexual behaviour of a person
 6) social services, economic support, social assistance and related social welfare services received by a person

9. Public data which can be released outside the statistical office without any protection limitation fall beyond these protection measures.

Data protection measures

10. The data protection measures are classified into 3 categories:

- basic protection
- additional protection
- intensive protection.

At least, the measures of basic protection are applied to material belonging to any of the data protection classes, additional protection is applied to class 2 material in addition to basic protection and intensive protection to class 3 material in addition to the above two measures.