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
(Skopje, The former Yugoslav Republic of Macedonia, 14-16 March 2001)

Working Paper No. 43
English only

Topic IV: Progress in the implementation of SDC methods and techniques in central and eastern Europe

STATISTICAL DATA CONFIDENTIALITY IN THE TRANSITION COUNTRIES: 2000/2001 WINTER SURVEY

Invited paper

Submitted by the ECE secretariat

I. INTRODUCTION

1. This paper presents the results of the survey on statistical data confidentiality in the transition countries, carried out by the UN/ECE secretariat in 2000/2001. The purpose of the survey was to review the development of statistical data confidentiality (SDC) in transition countries during last 2 years, to identify problems that need attention and areas where international cooperation could be more efficient in supporting the development. It is the follow up to a similar survey conducted in 1998 which was presented at the Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality in March 1999 in Thessaloniki, Greece. Some comparisons can therefore be made concerning progress in statistical data confidentiality in the transition countries during 1998-2001.

2. The following transition countries participated in the survey:

- **Eastern Europe** – Albania, Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, Slovenia, The former Yugoslav Republic of Macedonia, Yugoslavia (altogether 13 countries);
- **Commonwealth of Independent States (CIS)** – Armenia, Azerbaijan, Belarus, Kyrgyzstan, Russian Federation, Tajikistan, Ukraine (altogether 7 countries).
- In addition, Mongolia participated in the Survey.

The data for CIS countries and Mongolia are grouped together for the analysis.

3. The first section of the paper provides an overview of the state-of-the-art of statistical data confidentiality in the transition countries. It reviews the general confidentiality policy of the national statistical offices (NSOs), its legal basis, the comparative importance of the different aspects of confidentiality to statistical offices, and development in this area during the last two years.

4. The second section analyses in more detail the technical, administrative and organisational measures used for ensuring confidentiality. The last section provides an overview of the main problems with SDC in the transition countries and identifies possible future developments. Where appropriate, the paper also compares the situation two years ago (based on the 1998 survey). This is not always possible as the questions asked in the surveys in 1998 and 2000 are to some extent different.

5. The Annex to this paper, Working Paper No. 43/Add.1, provides a summary of individual replies to selected questions.

II. GENERAL OVERVIEW

II.1 Importance of statistical data confidentiality issues to statistical agencies

6. All the statistical agencies of the transition countries recognise the importance of the protection of statistical data. It is considered important or very important to the statistical agencies in all responding countries. Several statistical offices consider SDC and data protection among their priority activities. There is a slight difference in the approach towards data on natural persons and on enterprises, the protection of enterprise data seems to be slightly more important than the protection of personal data: 90% of the agencies consider the protection of enterprise data "very important", as opposed to 81% in the case of data on persons.

7. As opposed to western countries that are involved in SDC issues from the 1980s and even the 1970s, the transition countries only began to deal with this topic in the 1990s. This was, on the one hand, due to the economic, social and legal changes; and on the other hand, to the development of information and communication technologies, increasing use of PCs, databases and networks. For the moment, the pressure on the statistical offices of transition countries to release microdata is perhaps not as intense as in the western countries. However, the requests for more detailed data are expected to increase as the technology and market catches up with the more developed countries.

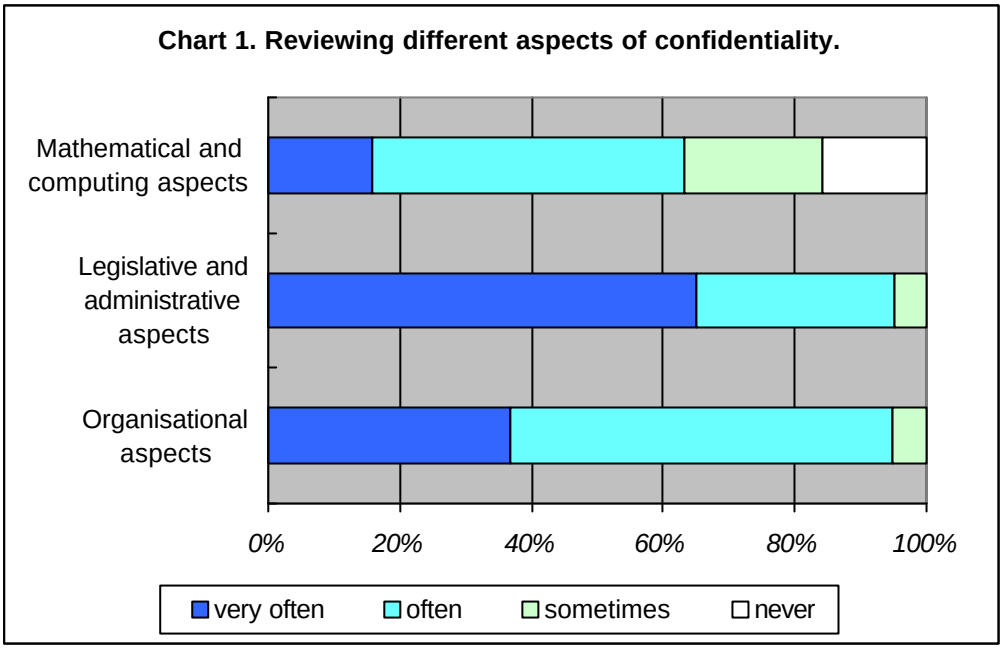
8. Increased attention to data confidentiality problems can, to a certain extent, also be due to the censuses: the Population Census 2000 and agricultural censuses conducted in some transition countries. The collection of huge amounts of personal data through the census always raises confidentiality concerns among the general public. The opposition in some countries shows that processing census data is a very delicate issue and of great concern to people. The increasing gaps between rich and poor and growing criminality in these countries makes the public attitude toward confidentiality very sensitive, especially concerning the protection of privacy of the individual.

9. The increased sensitivity towards censuses can be linked with the general uneasiness regarding modern information technology, and a lack of confidence that the data collected by a statistical agency will not be used by other government agencies (including police and tax authorities) for other than statistical purposes. The census allows the statistical agencies to see how their data collection activities may be perceived by the general public and politicians. A breach of confidentiality can have a damaging effect on the willingness of respondents to cooperate with statistical institutes. When respondents are obliged to complete a survey, the issue of mistrust in the statistical agency may affect the completeness and reliability of data.

10. At the same time, a census is a unique opportunity to discuss confidentiality issues on a nation-wide level, to review the principles of protecting confidential data, to assess the public attitudes towards confidentiality and to prove to the general public how the confidentiality promise is kept by the statistical office. The funds allocated for protecting the data collected by the population census can be used to improve the confidential data protection methods of the statistical agencies in general.

11. With regard to the different aspects of confidentiality, most attention is paid to the legislative and administrative aspects (Chart 1). Attention to all aspects of confidentiality has significantly increased over the last two years. Although the legal safeguards are in place in most of the transition countries, the changing circumstances, development of information and communication technologies and increasing public concern necessitate reviewing the legal basis of confidentiality from time to time. Based on the replies to the questionnaire, we can say that laws and rules on confidentiality are reviewed regularly in most of the countries.

12. Some areas where the legal basis and rules still need to be reviewed are confidentiality policies concerning enterprise data. Often, it might be necessary to have slightly different confidentiality policies for enterprises and private persons, and to redefine the rules for enterprise data at the legislative level. Another area where legislation can pose problems is the use of administrative data. In some cases, the use of registers may be forbidden by law because of the danger of disclosure.



13. The organisational and administrative safeguards are intended to reduce the risk of disclosure (like working on site, screening the users, screening the results with regard to disclosure control). Organisational aspects are also reviewed very often or often in practically all responding agencies.

14. Mathematical aspects receive less attention as was also the case in the previous survey in 1998. The technical (mathematical) measures aim to prevent disclosure by modifying data in such a way that disclosure is virtually impossible. It is agreed that the risk of disclosure can never be totally eliminated, therefore the aim of the technical safeguards is not a 100% guarantee against disclosure but to make data anonymous so that it could be re-identified with only an unreasonable amount of time, cost and manpower. Reasons for less attention to mathematical safeguards can be that there is not yet enough awareness in the transition countries, especially in the CIS countries and Mongolia, about different techniques that can be used to protect confidential data. The software is not readily available. Argus software was tested in some countries but was not always usable because of the prevailing circumstances (e.g. different alphabets).

15. Here a general remark has to be made concerning the relation between statistical confidentiality and data protection. There is quite a lot of confusion around the terms “data protection”, “security”, “disclosure” and “confidentiality”. Data protection is a more general term covering the measures for the protection of personal data “against accidental or unauthorised destruction, or accidental loss, as well as against unauthorised access, alteration or dissemination” (Convention for the protection of individuals with regard to automatic processing of personal data, Council of Europe 108/81). Confidentiality is a specific sub-area of data protection, namely avoiding disclosure of personal data, such as identification. Common terminology (definitions) in this area would be desirable.

16. In data collection and processing, data protection and confidentiality are often linked. Data can be physically destroyed or distorted, but also individual data can be identified. Methods that are used are basically data protection methods. The statistical office has a responsibility to ensure that unauthorised persons cannot access individual data.

17. In the data dissemination process, data protection and confidentiality are also linked – with an emphasis on confidentiality. However, confidentiality continues to apply after the data has been released and the statistical office does not have any influence over the data anymore. The data has to be such that re-identification of respondents is practically impossible, whatever the user does with the data.

18. Based on the replies to the questionnaire, it is often assumed that anonymity (omitting identification variables) is sufficient to avoid disclosure. The disclosure of personal data means establishing a one-to-one correspondence between the record and a specific individual. This can also happen when the direct identifiers are omitted, e.g. through linkage of the data via key variables in two or more different datasets. Risks are increased when, for example, a person was interviewed for a particular survey (which makes identification easier) or recognising rare persons (which can occur by accident).

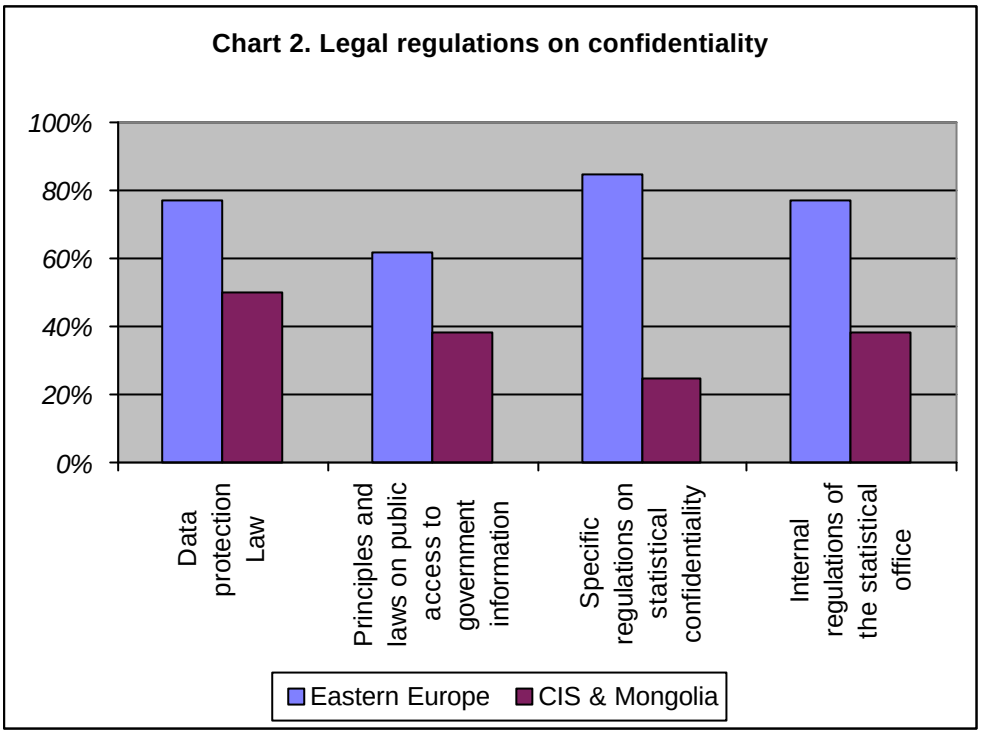
19. Possible re-identification of respondents does not apply only to microdata but also to tabular data. When releasing data with breakdown according to industrial branches or small geographic areas, some table cells can contain data about only one or few business units from where the respondent can be identified directly or using some additional data that can be available from other sources.

20. In many offices, data protection is done on an ad hoc basis in different statistical areas. Unified management and policy decisions at the agency level are required to lay the foundation for a systematic approach towards confidentiality to manage together the legal, IT and organisational aspects. It is the responsibility of the management to create the necessary awareness of confidentiality problems and to manage the preconditions for efficient solutions on organisational, methodological and technical levels.

II.2 Legal basis

21. The legal basis for confidentiality is established in most transition countries. Special attention to these questions has been paid in the so-called candidate countries planning to join the European Union (Bulgaria, Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovak Republic and Slovenia). Most of these countries have adopted or updated their statistical laws in the last two years to comply with the requirements of the European Union in the area of confidentiality. More details about the legal basis for confidentiality in the candidate countries can be found in Working Paper No. 32 (by Dobrinka Borisovska Gospodinova, The former Yugoslav Republic of Macedonia).

22. In most of the countries, the statistical offices' responsibility to guarantee confidentiality of data is stated in the Law on Statistics. Other regulatory acts dealing with confidentiality are the data protection law, principles and laws on public access to government information, specific regulations on statistical confidentiality and internal regulations of the statistical office. 77% of the east European transition countries and 66% of the responding CIS countries have a data protection law. In 85% of the east European countries and in 33% of the responding CIS countries confidentiality is also covered by specific regulations of the statistical office. All legal regulations were adopted in the 1990s, and mostly during the second half. Several laws have been updated and amended in 2000/2001. The graph below shows the percentage of countries that have adopted a specific law or regulation. It is difficult to make a one-to-one relationship between the specific laws and regulations of confidentiality in different countries as the same aspects of confidentiality can be regulated either by a data protection law, law on statistics or other laws on public access to government information.



II.3 General policy of statistical offices towards confidentiality

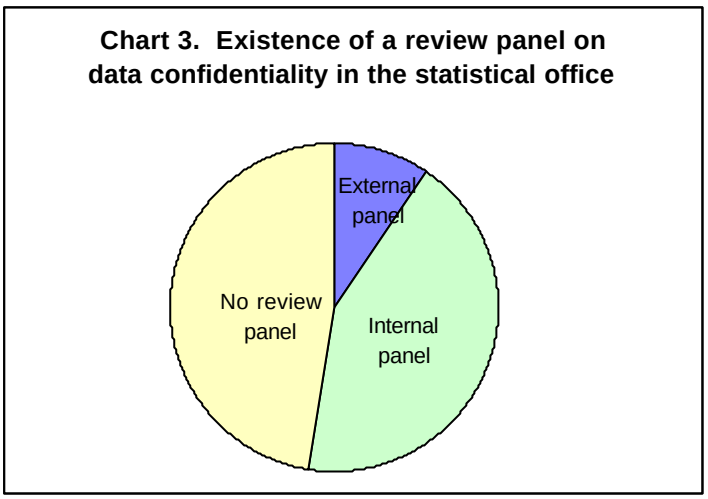
23. This part touches on some specific issues that give an overview of the policy of statistical institutes towards confidentiality, such as allowing access to original data, assessment of public attitudes, existence of a review panel on confidentiality, informed consent and sensitive data items.

Assessment of public attitudes

24. Compared to the situation two years ago, the statistical offices are more aware of the importance of the attitude of the general public and the respondents towards statistical confidentiality. The assessment of public attitudes, perceptions and reactions to confidentiality is not conducted only in four countries (Romania, Azerbaijan, Kyrgyzstan and Ukraine) which is considerably less than in 1998. 46% of the east European countries assess public attitudes often or very often while all the responding CIS countries conduct such an assessment sometimes or not at all. Mongolia conducts assessment of the public attitudes towards confidentiality often.

Staff responsible for confidentiality

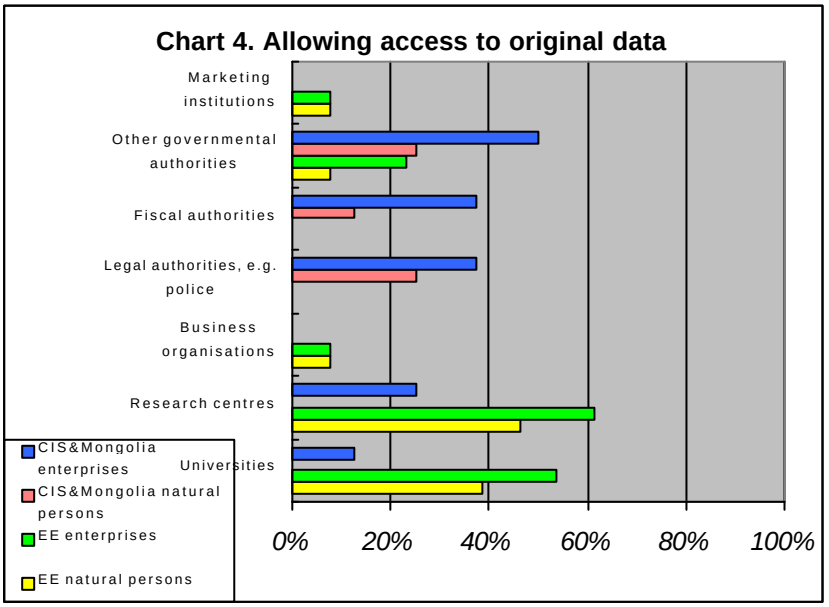
25. In 1998, about half of the responding countries used a review panel to judge whether the statistical data are sufficiently safe for outside users. This time, 52% of the respondents use a review panel, which in all cases except Albania and Lithuania, is an internal panel. In 1998, Hungary was the only country with an external review panel. The percentage of statistical offices in the transition countries who have a confidentiality review panels considerably increased (38% in 1998).



26. 46% of the east European countries and 25% of the CIS countries together with Mongolia have special staff in the statistical agency who are responsible for data confidentiality in the office.

Allowing access to original data

27. In general, the statistical offices are not willing to allow access to original data to other institutions. The situation has somewhat changed during the last two years. 29% of the responding countries do not allow any access to original data to other institutions. In 1998 this figure was 47%, so we can observe here a tendency towards increased openness. The attitude is more cautious concerning the data on natural persons: 7 east European countries (54%) and only 2 CIS countries (25%, Tajikistan and Ukraine) allow access to external institutions to original data on natural persons.



28. Access is allowed mostly to universities and research centers, and only for statistical or research purposes. The only exceptions to this are Bulgaria (access allowed to other governmental authorities), Lithuania (access allowed to business organisations and marketing institutions), Tajikistan and Ukraine (access allowed to legal and other government authorities, also to fiscal authorities in Tajikistan).

29. Providing access to original data on natural persons to universities and research centers has considerably increased in the east European countries (25% in 1999, 54% in 2000). This can be the result of pressure from the research community to have access to more and more detailed data for their analysis. On the contrary, in the CIS countries and Mongolia practically no access to original

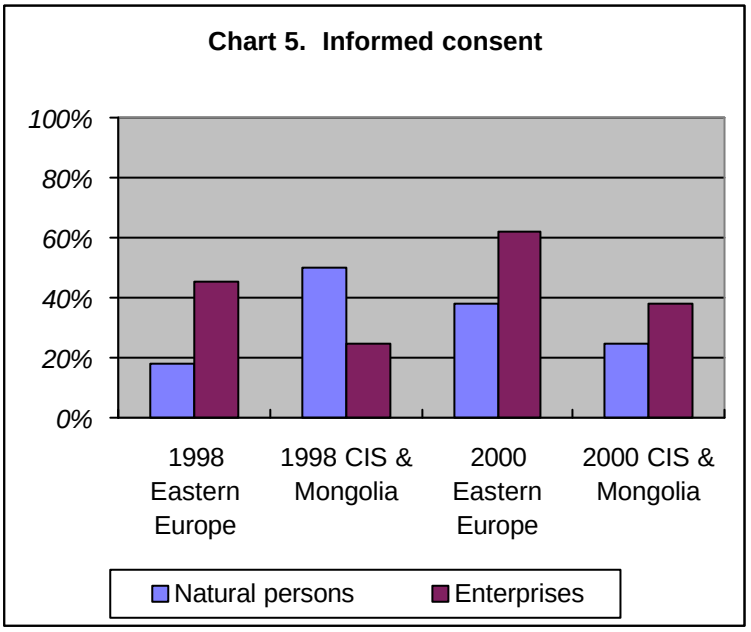
data on natural persons is allowed, except for Tajikistan and Ukraine where access is allowed to government agencies but not to research institutions and universities.

30. Access to the original data on enterprises is provided more frequently. 9 east European countries (69%) and 5 CIS countries (63%) allow access to original data on enterprises. No access is allowed in Azerbaijan, Belarus, Hungary, Mongolia, Poland, Slovenia and Yugoslavia. Similarly with personal data, in the east European countries, the institutions that can access the data are mostly only universities and research centres. The exceptions are Albania, Bulgaria and Czech Republic (access allowed to other governmental authorities) and Lithuania (business organisations and marketing institutions). In the CIS countries the situation is a little bit different than with personal data. In Kyrgyzstan, Tajikistan, Russia and Ukraine, the access to original data is allowed to legal, fiscal and other government authorities (including police), even more easily than to universities and research institutions.

Informed consent

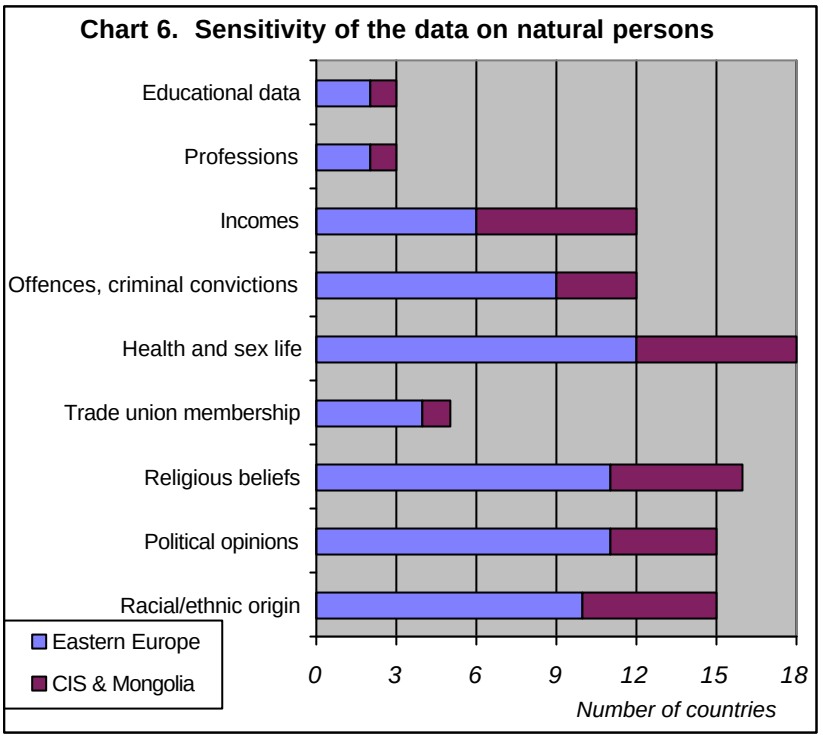
31. Informed consent is used much more often than two years ago, and there is also a difference in this sense between the east European and CIS countries. When in 1998, natural persons could authorise the disclosure of original data in only 25% of the responding countries, in 2000 this percentage was 33% (38% in east European countries and 25% in CIS countries). Informed consent is used a little more frequently for enterprises than for natural persons (Chart 5).

Chart 5. Informed consent



Sensitive data

32. Concerning the sensitivity of the data on natural persons, the most sensitive data items are health and sex life political opinions, religious and philosophical beliefs, and racial and ethnic origin. Data relating to offences, criminal convictions and security measures, and data on incomes are also quite sensitive. The data on incomes is considered sensitive in about two thirds of the transition countries (one half in western Europe). From all the 21 responding transition countries, information on professions and education is considered sensitive in Albania, Bulgaria and Ukraine. Here is an interesting discrepancy with the EU where in about half of the countries these data items are also considered sensitive (according to a similar survey conducted on Eurostat's behalf in 1997). The statistical offices of Azerbaijan and Yugoslavia have not yet determined what kind of personal data should be considered sensitive.



33. Concerning sensitive data on enterprises, in most countries all data relating to an individual enterprise are considered sensitive, except identification data (name, address, etc.) or other data that are exceptionally treated as public by law. This is the case in 67% of the responding countries. Sometimes an exception is made for data on the profile of activity (Czech Republic), legal form, social capital, turnover and number of employees (Romania), kinds of activity, number of staff, kinds of products and environment pollution (Latvia and Lithuania). In Tajikistan, on the contrary, only data on those enterprises that deal with precious metals or military production are considered sensitive.

34. The approach of considering all enterprise data confidential by default can pose a problem in many countries when releasing any detailed data on enterprises. Often a particular company is the only producer or one of the very few producers of certain products. The problem is more acute in smaller countries but is valid also for bigger countries, east European countries as well as west European countries. Some countries (e.g. Armenia) have a special clause in the law that in the case of a monopoly, the data about that particular enterprise are not confidential.

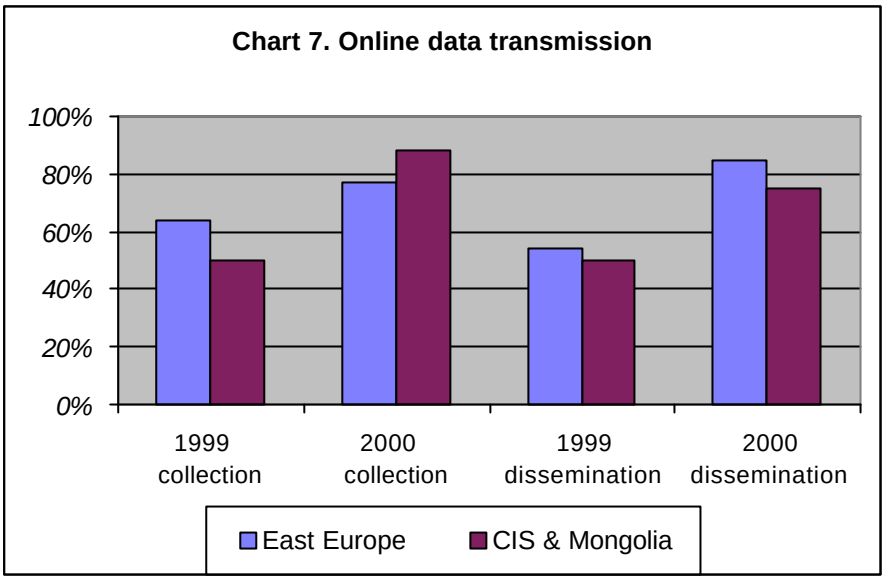
35. Another problem is that often because of confidentiality the statistical office cannot release data that are freely available from other (government) sources (such as quarterly, annual reports, balance sheet data).

36. In general, there is no big difference between the treatment of the data on individuals and data on businesses. The differences are due rather to the nature of data and not to a fundamental difference in policy. However, it might be necessary to make such a distinction even on the legislative level, as in the case of enterprises, confidentiality rules that are too strict can hinder the dissemination and exchange of data. It might be necessary to reconsider the prevailing approach that all data about enterprises are confidential.

Online data transmission

37. One of the areas that require specific measures of data protection is online data transmission. Online data collection has increased over the last two years. Data are collected online (at least sometimes) in 81% of the responding transition countries (as opposed to 60% in 1999). Albania, Bulgaria, Romania and Azerbaijan never collect data online. Concerning the frequency of online data

collection, most countries have responded “sometimes”, only Poland and Mongolia collect data online often.



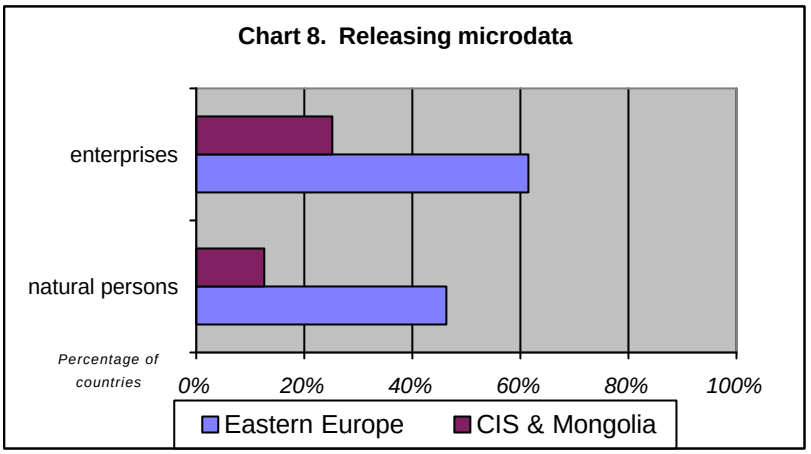
38. Online data dissemination has also been increasing: data is transmitted online to clients (at least sometimes) in 81% of the countries (as opposed to 53% in 1999). Latvia, The former Yugoslav Republic of Macedonia, Russia and Ukraine never disseminate data online. It is done very often in Azerbaijan, Poland and Mongolia, often in Bulgaria, Romania, Armenia, Belarus, Kyrghyzstan and Tajikistan, and sometimes in all other countries not mentioned above.

III. CONFIDENTIALITY PROTECTION MEASURES USED

III.1 Forms of data release

39. In order to avoid disclosure, often an easy solution is not to release microdata at all. Therefore, several transition countries are very reluctant to release any microdata. Out of the 21 responding countries, 14 do not release microdata on natural persons and 11 do not release microdata on enterprises. Bulgaria, Czech Republic, Estonia, Poland (except the Labour Force Survey), Yugoslavia, Azerbaijan, Belarus, Russia, Tajikistan, Ukraine and Mongolia do not release any kind of microdata. Looking at data on natural persons and enterprises separately, 46% of the east European countries and 13% of the responding CIS countries and Mongolia release microdata on natural persons and 62% of the east European countries and 25% of the responding CIS countries release microdata on enterprises.

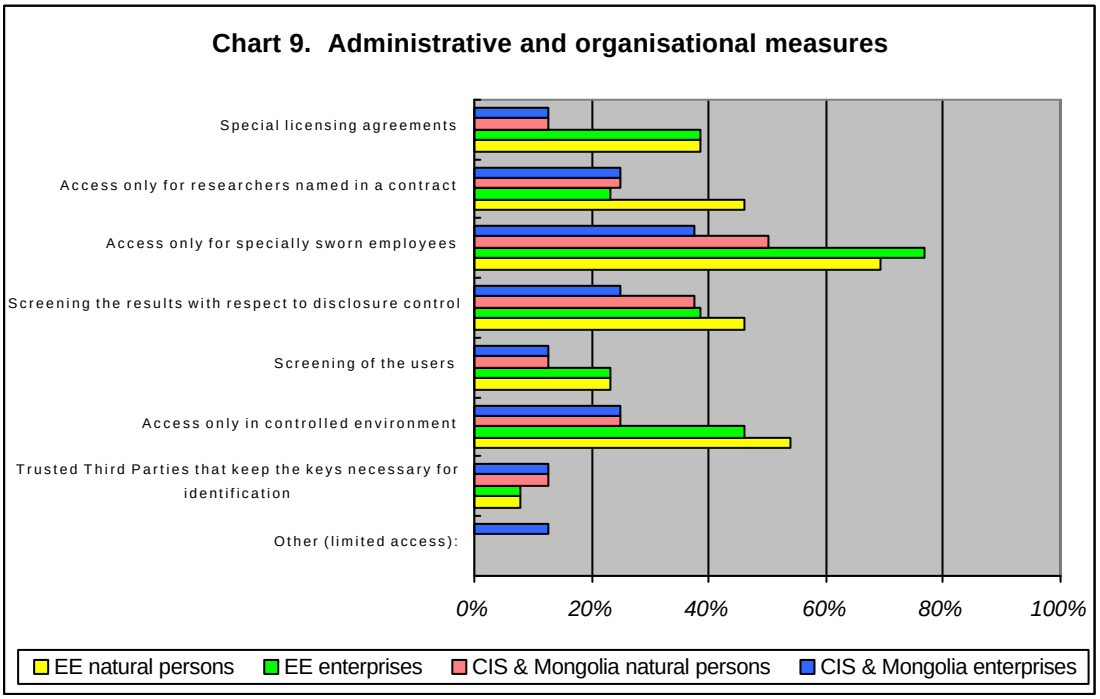
40. The forms of release of microdata that are more often used are microdata for research and synthetic data files. The public use files (PUF) are used to some extent for data concerning enterprises. These forms are used in 52% of the responding countries. No other forms of microdata release are used.



III.2 Administrative and organisational measures

41. As stated in the introduction, the legislative and administrative aspects receive the highest attention from statistical offices. With the exception of Slovenia and Belarus, all countries use some kind of organisational measures to prevent access of unauthorised persons to confidential data and to ensure that no confidential data is distributed outside the office. In many agencies, especially in the CIS countries, the administrative and organisational measures are the main safeguards for confidentiality, linked with general measures for protection of data from unauthorised access, distortion or loss of data.

42. The organisational and administrative measures most often used are allowing access to only specially sworn employees. About 70% of east European countries use this method. The access to data by regular employees is not considered data release or dissemination. Specially sworn employees are subject to the same legal conditions as the statistical institute staff. They are temporarily given restricted access to the data on the same grounds as regular employees of the office, usually on site. All the data released as a result of such activities is covered by the usual confidentiality restrictions.



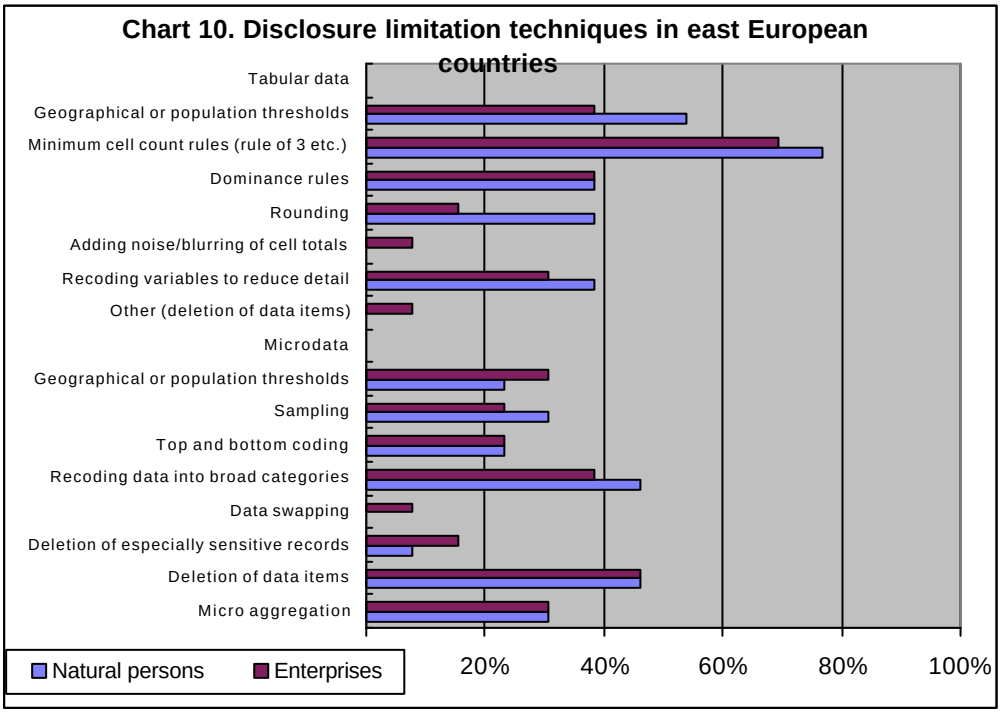
43. Other measures that are used more often are: access only in a controlled environment, screening the results with respect to disclosure control, and access only for researchers named in a contract. Several of these measures make the persons working with the data personally responsible for ensuring confidentiality. With specially sworn employees, licensing agreements and special contracts often the same restrictions to data use and the same liabilities apply with the same kind of penalties for breaching confidentiality as for the staff of the statistical office. In most of cases, the purpose of data access must be clearly specified and the statistical office reserves the right to refuse access to original data.

III.3 Disclosure limitation techniques

44. The disclosure limitation techniques that are used most often in east European countries can be seen in the chart below. The most popular methods are: minimum cell count rules (data are not released if they are composed of less than a certain number of respondents, usually 3); geographical or population thresholds (releasing data only for areas above a particular spatial or population threshold); recoding data into broad categories and dominance rules (if fewer than a certain number of units (usually 2-3) account for a certain percent or more of the cell total (usually 80%)).

45. Practically all east European countries use some kind of disclosure limitation technique, and mostly several techniques combined. Although there is a general problem with the lack of specialised software, countries have either developed in-house software for this purpose, or implement these techniques manually.

46. Concerning the CIS countries and Mongolia, specific disclosure limitation techniques are seldom used. Some implementation of these methods has been reported by Armenia (micro-aggregation), Kyrgyzstan (recoding data into broad categories, data swapping and micro aggregation). An exception here is Ukraine where practically all methods for tabular data protection are used.



47. The detailed confidentiality rules and critical values used by the agency in implementing the above techniques are made public in about half of the east European countries and in Azerbaijan.

IV. MAIN PROBLEMS AND POSSIBLE FUTURE DEVELOPMENTS

IV.1 Major challenges

48. Technical assistance is required in all areas (methodology, organisation, software, training) but the most frequently mentioned issues were software and training. Progress in the area of methodology and mathematical methods of SDC is limited because of the limited capacities of the statistical offices and the complexity of the methods.

49. Training staff and then retaining the trained staff in the office is a general problem in statistical offices in all areas of speciality. The salaries in the statistical office are often not compatible with the private sector and statistical offices therefore have to find other means (such as career perspectives, interesting work, etc.) to keep highly qualified personnel. As the area of confidentiality, especially its mathematical methods and software, is relatively new to the statistical offices of the transition countries, the additional complexity is that as the technical know-how is not available in the country, the only possibility is to get specialists for training from other countries.

50. One of these particular areas is confidentiality software linked with database management systems, which is also a problem in more developed countries. The increasing possibilities to combine data from different sources, cross-tabulation, matching, record linkage, etc. raises the need for tools able to ensure confidentiality in these conditions. The database management systems do not include tools for confidentiality protection, which is a great disadvantage in their use in statistics. Special attention is needed to disclosure control for confidential data from administrative registers and data sharing agreements with other agencies.

51. The attempts of computer hacking of the sites of national statistical offices, or of the data flows between the statistical office and data providers have not yet posed major problems in transition countries. But this situation can be expected to change and attention has to be paid to data protection against hacking. Some offices note that such cases are becoming more and more frequent. Mathematical methods are needed to protect data during their transfer via networks and improve the quality of software to identify hacking and to protect the stored data.

52. Several countries highlighted the need to raise awareness about the issues of statistical confidentiality among the staff of the office as well as among the general public. Especially in cases where there are statistical production units in the state ministries, there can be (political) pressure to make available microdata for certain government officials who are not sworn to secrecy.

53. A few countries receive technical assistance with the implementation of SDC, namely Bulgaria (Argus software), Poland (consultation and training from Eurostat and University of Ulm), Latvia (consultations from Statistics Sweden and cooperation project with Statistics Denmark) and Russia (from Eurostat and Statistics Finland). In addition, the participation in confidentiality meetings has been financed from PHARE (for the 1999 meeting) and TACIS funds.

IV.2 Future developments

54. Concerning future projects, 62% of the east European countries and 50% of the CIS countries have plans for specific projects focused on confidentiality. Projects on general data protection and network security, such as replacement of LAN servers and equipment, etc. are excluded. Confidentiality related future projects are mostly dealing with software, either studying possibilities to use special software (Bulgaria, Hungary) or the implementation and testing of software (e.g., Czech Republic plans to test Argus). Other plans concern the legal basis (Albania), analysis of the general situation of confidentiality and improving coordination between government bodies in the area of confidentiality (Bulgaria, Romania), training and consultation (Bulgaria, Latvia, Ukraine). Slovakia is in the process of implementing an Automated Statistical Information System, which also includes measures for confidentiality protection. Belarus is planning to elaborate the rules for confidential data protection in the Ministry of Statistics. Russia is conducting a project "Confidentiality of statistical data" within the framework of a TACIS programme.

55. Even when the statistical offices will have established a reasonable balance between the data users' need for detailed data and the data providers need for privacy and confidentiality, the statistical offices need to be aware of the risks of disclosure of statistical data which may arise as a consequence of IT development. Some future trends that can be foreseen in the development of SDC in the transition countries are the following:

- Increasing pressure on statistical offices to release microdata due to developing markets and technical progress. On the one hand, demand for more detailed data is created by increasing market competition and the need to analyse the influence of government decisions on the economic and social situation. On the other hand, the capabilities for detailed analysis are created by improving technology and emerging institutions that are specialised in such research (e.g., market analysis);
- (Temporarily) increased attention to confidentiality, both from statistical offices and the general public, because of the population census – both a challenge and an opportunity to improve SDC protection;
- Increased danger of computer hacking because of the increasing use of Internet for dissemination, e-government initiatives and government wide Extranets;
- Need to review the legal basis:
  - to make it compatible with EU regulations;
  - to specify different handling of data on physical and legal persons;
  - to overcome conflicts in laws concerning data on legal persons that can be released by the statistical office and that can be released by other (governmental) organisations (e.g. balance sheets, quarterly, annual reports released by enterprises);
  - concerning use of data from administrative registers;
- Need to move from ad hoc solutions in individual statistical areas to developing an agency policy concerning confidentiality of disseminated data;
- Confidentiality in relation to the quality of statistics will require attention. Confidentiality can be regarded as an important quality dimension, on the other hand, preserving confidentiality makes necessary compromises between confidentiality and precision, coverage, etc.;
- Data warehouses and integrated statistical information systems are beginning to develop in the transition countries. The high volume of confidential data available in these systems makes it necessary to review the production environment from a confidentiality perspective. The dramatically extended possibilities to combine data from different sources, record linkage and matching, etc. raise the need for tools able to protect confidentiality in these conditions. Particular danger lies in the public use of anonymous microdata for analytical work because of the very high risk of disclosure. The impact of these developments is not yet very visible in the statistical offices of the transition countries but it can be expected to have an influence in the near future.