CONFERENCE OF EUROPEAN STATISTICIANS

Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality Session 1.1

29-31 October 2019, the Hague, the Netherlands 14 June 2019

Abstract on Data Confidentiality in ICBS Research Rooms

Julia Vider (CBS, Israel)

juliav@cbs.gov.il

Abstract

The main task for the Israeli Central Bureau of Statistics (ICBS) is produce statistics about the Israeli society. In order to do this ICBS collect and process a substantial amount of data on persons and enterprises, many of which are of a confidential nature. It is therefore essential for ICBS that all data on individual citizen and business enterprise are treated in the strictest confidence. These rules as laid down in legislative framework and in ICBS data confidentiality policy that specifies how to ensure this protection.

The extensive collection of data contains a substantial research potential about the Israeli society. Therefore, the ICBS gives access to microdata for researchers and analysts, for well-defined research project under well protected conditions. There is an increased interest of researchers to work with Microdata files. Microdata files for research purpose are available to researchers in three levels of confidentiality classification files: Public Use Files (PUF), Microdata under contract Files (MUC) or as research room files (RRF). PUF are standard anonymized microdata products made available to the public at large subject to a standard CBS license. Due to data security and confidentiality reasons, the researchers work on MUC and RRF only in research rooms. These Files are de-identified detailed microdata where only minimum disclosure control has been applied. Therefore, work in research rooms is restricted to academic researchers and researchers from research institutions upon approval of their institution and their research proposal by the Chief Scientist of the ICBS. All researchers using the research room undergo a security check, and are subject to criminal sanctions for breach of confidentiality. Physical and legal protection in the research rooms is achieved by the establishment of secure environments in dedicated research room facilities hosted by ICBS, project agreements and confidentiality statements between the researchers and ICBS. General rules for data security are: • Data provided to researchers by "need to know" principle. • Data anonymized - unique key for each project. • No attempts to identify people or enterprises – or to remove microdata must be made and is considered a very serious breach of the agreement between the researcher and ICBS. • Only aggregated data, where no identification of persons or enterprises is possible, can be removed from the protected environment and only after approval by output inspectors at ICBS. Prevention of disclosure entails a shared responsibility of ICBS and the researcher. Therefore, output inspectors at ICBS evaluate all output carefully on disclosure before it can be released to the researcher.

We have prepared Guidelines for transferring output from the research rooms to researchers in order to clarify what type of information is allowed to be exported as an output. • No microdata in any form must be released. • All tabular and similar output from surveys should have at least 5 units (unweighted) underlying any cell or

data point presented from survey data or from administrative files. • In all tabular frequency tables and similar output no cell can contain more than 90% of the total number of units in its row or column to prevent group disclosure.

We are facing a lot of Data Confidentiality issues and would be very interested to share our knowledge and learn about other data confidentiality methods.