

Rules of Statistics Finland's Research services

Terms of use and obligation to secrecy

Statistics Finland may release or grant permission to use confidential data collected for statistical purposes for scientific research and statistical surveys on social conditions. Data may not be used in an investigation, surveillance, legal proceedings, administrative decision-making or other similar handling of a matter concerning an individual, enterprise, corporation or foundation. The research use of Statistics Finland's unit-level data files requires a user licence, which must be valid throughout the processing of the data files. Only the person who has been granted a user licence is permitted to use the data files subject to licence and the data files can only be used for the purpose accepted in the decision granting the user licence. A user licence is granted for a fixed period (at most for five years at a time).

Statistics Finland may release or grant permission to use confidential data collected for statistical purposes from which the possibility of direct identification of a statistical unit (person, enterprise) has been removed. By virtue of Section 19 of the Statistics Act (280/2004), data on age, gender, education, occupation and socio-economic group may also be released with identification data. Statistics Finland may release data on causes of death with identifiers based on the Act on the Openness of Government Activities.

The researcher responsible for the project applies for a user licence. In the application a user licence is applied for all project researchers who intend to handle or view unit-level data files. The licence applicant is under obligation to ensure that other persons having been granted a user licence in the project are aware of and comply with the conditions governing authorisation for the use of statistical data. If the person/persons having been granted a user licence should change or transfer to another organisation and wish to continue the research there, the licence application must be updated.

It is directed in the user licence that the data must be handled as confidential and no attempt must be made to identify the data subjects from the data. The material to be published must be protected so that no individual persons or enterprises can be identified. The persons concerned or their relatives may not be contacted on the basis of data released with identification data (Section 19 of the Statistics Act, or documents concerning the establishment of cause of death).

Each researcher handling unit-level data files must sign a pledge of secrecy. In the pledge of secrecy, the researchers pledge not to disclose to outsiders any information that they are legally obliged to keep secret. The obligation to secrecy also includes a prohibition on wrongful use of a

confidential document or information for personal or another person's gain or to injure another person.

A sanction is prescribed for violating the provisions on secrecy, non-disclosure and prohibition of use of the data. The punishment from these offences for researchers can be a fine or imprisonment for at most one year. Use violating the licence or breaching against the rules has an effect on the rights of the organisation and/or researcher to obtain a licence to Statistics Finland's data files in future.

After the end of the validity of the user licence, the researcher no longer has access to the remote access system and the data materials released outside Statistics Finland must be returned or destroyed after the expiry of the user licence. All copies taken and intermediate files formed of the data must also be destroyed. Statistics Finland must be notified about their destruction. The obligation to secrecy also applies after the validity of the user licence ends. It is possible to apply for a continuation of the user licence with an application for a user licence.

The released final products or their reference information must be sent to the contact person at Statistics Finland. When the results are published, Statistics Finland must be quoted as the source.

FIONA remote access system

Organisation level rules

Data other than those mentioned in Section 19 of the Statistics Act (age, gender, education, occupation, socio-economic group) and cause of death data must be handled in Statistics Finland's remote access system. The organisation of the researcher working in the FIONA remote access system must have a remote access agreement with Statistics Finland. An account of data protection and data security practices related to remote access use must be submitted to Statistics Finland as an appendix to the agreement. The agreement specifies the contact persons responsible for administrative and technical matters relating to the remote access use of the organisation. The contact persons must inform Statistics Finland of any changes in data protection or data security within the organisation which are of significance to the remote access use.

The person who signs the agreement on remote access use of research data files on behalf of the institution/organisation is responsible for the researchers in the institution working in the FIONA system. He/she is also responsible for that the researchers work in spaces approved by Statistics Finland and data files can be processed there so that the privacy of the data file is not compromised.

Processing the data files in the remote access system

Before the researcher can process a research data file in the FIONA remote access system, the researcher must sign a remote access commitment. In the remote access commitment, the researcher defines the modes and places of work and agrees to follow the rules related to remote access work.

Remote access is intended only for the use of the researcher who has been granted a permission to use the data and it must only take place in the premises mentioned in the remote access commitment, the IP address of which has been checked and approved by Statistics Finland. When the employer and/or premises change, the researcher must submit a new remote access commitment. Researchers must commit themselves to ensuring that both computers, networks and work premises are data secure. If they want to work from home, it must be made sure that the work can take place with a VPN connection through the employer's network. The mobile phone on which the DuoMobile application for identification in the remote access system is installed must be stored carefully.

The remote access system must only be used for the purpose mentioned in the user licence and its functioning must not be hindered in any way.

Researchers must ensure data protection during the research use of their data file and when publishing research outputs. The data must be handled so that the information in the data file will not become known to a third party, so the data on the screen must not be shown, shared or copied (e.g. a screen capture or a photograph). Protected personal identifiers or Business IDs must not be written in an email message, for example. Sharing the display of the remote access system in a remote meeting (e.g. Teams) is not allowed for data security reasons even if each participant in the meeting has a user licence to the data and/or there are no unit-level data subject to user licence visible on the screen. The remote device must be locked when it is left unattended and the device is not supervised, and the user must log out from the system when no longer working with the remote access.

The researcher must ensure that the research results requested to be exported from the system contain no unit-level data or possibility for their disclosure. (e.g. shnro personal identifiers). The guidelines related to data protection in the Research services must be followed in research outputs (tables, analysis results, graphics, etc.). Software files and files containing results can be sent by email only via Statistics Finland's personnel from the address tutkijapalvelut@stat.fi / mikrosimulointi@stat.fi. More detailed data protection guidelines can be found in the data protection guidelines for FIONA:

https://www.stat.fi/static/media/uploads/tup_en/mikroaineistot/fionan_tieto_suojaohjeet_en.pdf

If the researcher or customer breaches the agreements or instructions on remote access use, the remote access connection is shut down.

Granting a licence to use indirectly identifiable personal data in actual fact means releasing of personal data. Thus the holder of the licence becomes the data controller concerning those data, and is responsible for fulfilling the obligations set in the general and special legislation relating to the processing of personal data.