
Friday 15th January, 2021, 13:00

SDCC and DST forskerservice

This is a reminder and clarification of the rules we must obey when working with the (pseudo-)anonymized registers on the servers of Statistics Denmark (DST).

It does *not* replace the guidelines available at DST's website, <https://www.dst.dk/da/TilSalg/Forskningservice>, in this case primarily the notes for export of results from the DST servers, <https://www.dst.dk/ext/3477468153/0/forskning/Guidelines-for-transferring-aggregated-results-from-Statistics-Denmark--pdf>

You must stop reading this till you have read the DST guidelines.

Transferring data

The guidelines from DST stress what you are allowed to transfer via the send-home system at the DST servers.

But you should be aware that this system is also the *only* means you are allowed to use to transfer data. It is *forbidden* to

- make screen-shots of the screen against the DST-server on your own computer
- take pictures of the screen with your phone or camera
- read results off the screen and write them on paper or in a file; the argument here is that this in principle is the same as using a camera, albeit one of a terribly low quality

This means that if you are using data or graphs in your manuscripts they must be put in a file at the DST server, complying with the rules, and sent via the DST system to your email. You cannot use the results until then.

The rationale is that anything you extract from DST should be subject to monitoring by DST—every time you send a file from the DST server to your own mailbox, DST will have the possibility to check that it complies with the rules.

In short: You can *only* use results that are in a file you exported from DST.

Internal communication about microdata

If you have specific data processing problems that require a listing of microdata to understand, you can make one, but *you must leave the results on the DST server*. You can then ask a colleague with access to the same project to look at the data listing and help you with the problem. Delete the listing afterwards to avoid accidental breach of rules. This way everything is kept inside the DST servers.

You cannot share screens via Teams or Zoom or similar if you have an open connection to the DST server.

If you violate the rules...

...you must *immediately* contact the register responsible person, Birgitte Broch, or even better the persons with daily oversight of the DST contact for your project.

For the Clinical Epidemiology project 707655 it is [Else Ibfelt](#) or [Dorte Vistisen](#). If not available you may try [Bendix Carstensen](#) or [Pernille Falberg Rønn](#).

Scientific implications

The following is not mandatory but useful advice that can be painful in the short run, but may be like an epiphany once you learned it.

Whether you use SAS, Stata or R make sure that you have a machinery that allows your programs to produce files that contain *both* the code and the results from the code.

If you work in R you may use R-weave or R-markdown to produce `.pdf`, `.html`, `.tex` or `docx` files that you can export to your mail system.

If you work in Stata you may use MARKSTAT or MARKDOC to produce `.pdf`, `.html`, `.tex` or `docx` files that you can export to your mail system.

If you work with SAS you can either run SAS in batch that directly will produce plain text files with extensions `.log` and `.lst`—see section 3.2 on p. 16 of

<http://bendixcarstensen.com/DMreg/DMreg2018.pdf> for a description. Otherwise you must manually save the program log to a `.log` file and the output window to a `.lst` or `.html` file.

There are no requirements from DST that you behave in a scientifically responsible way, but it is a good idea to groom your programs to produce the right and only allowed amount of output, then you will have a set of files where all analyses are documented. You are allowed to send even slightly revised versions of previously sent files as often as you like.

If you get into the habit of always making programs that produce well-defined analysis results in a transferrable format you minimize the risk of accidental breach of rules.