STATISTICS DENMARK

March 2022

Division of Research Services

Rules for data safety under the microdata scheme hereunder rules for transferring analysis results and sanctions in case of data breach

Content

Introduction

Statistics Denmark makes our many valuable data available to users who have a well-founded desire to analyse data for the benefit of Danish society. It is important that this is done in a way where both data security and data confidentiality are of the highest standard. The individual citizen and company are entitled to have their confidential data treated with the utmost care. The general rules for the processing of confidential data are laid down in the EU Regulation on the protection of personal data (General Data Protection Regulation)

Data confidentiality is a key prerequisite for the existence of microdata schemes. All data sets accessed through the research scheme are confidential. Therefore, as users — through agreements with Statistics Denmark — you commit to obtain only general results and *not personal or* individual data from the research machines at Statistics Denmark.

Below is a description of the main rules on how to work with data on the research machines/hosted machines, the transferring of files, including what is meant by microdata and detailed tables, the procedure for breaching data confidentiality, as well as some advice on how to avoid breaches. At the end of the guide you will find an overview of some general examples of types of data breaches.

The rules described in this guide are a simplified version of the rules contained in Statistics Denmark's data privacy policy. In case of transfer of results under the microdata schemes, the rules as described in this guide apply.

Access to the research machines and work with data

Before accessing data under microdata schemes, there are certain basic conditions that must be met. We require that the institution that applies for access to microdata must be authorised, i.e. the institution must be approved by Statistics Denmark to be able to access microdata for specific projects. In addition, all users must approve a user agreement. When a user approves the user agreement, the user confirms to be familiar with the data security rules, i.e. that the user is familiar with what to do and what is not allowed when you have access to confidential data. Finally, the person responsible for the authorisation of the institution or his representative must also approve a contract of attachment. Approval of the attachment agreement confirms that the institution takes the data security responsibility for a user's access to pseudonymised data on the research machine. These agreements are set out in Appendix 1 and Appendix 2.

Accessing data under microdata schemes gives you access to data under a project number. It can be a specific project, a project database or a public sector scheme

Common to these projects is that the data accessed contains confidential information. Access to data is therefore protected with personal passwords.

The passwords obtained for accessing data on the research machines are personal and may not be given to others

You must never hand over these passwords to others. This also means that you must not leave or leave your computer to others when you are logged in to your project on the research machines. Even if they themselves have approved access to the same project. An authorised access means that a user has approved a user agreement, has been assigned to the institution through an approved affiliation agreement and has accessed the data of the specific project.

If you have to leave the screen for a shorter or longer time, access to the research machine must be interrupted (you log out) to ensure that others cannot access. It is therefore not enough to put a screensaver on — access to the research machine must be completely interrupted. If you suspect someone else knows your password, you need to change your password as soon as possible.

Where to work with access to microdata?

You are only allowed to work with microdata under the microdata schemes, in the following locations:

- At the workplace, i.e. the authorised institution
- Via a home workplace

The above rules also mean that you are not allowed to work with data in public places, e.g. in libraries, cafes or on the train.

Working with microdata — what is allowed?

It is allowed to both view and work with microdata on the screen. For example, it is relevant to look at a small sample of microdata if, as a control, you have to see if the formation of a new variable has gone well. But you must never try to identify individuals — not even yourself.

It may also happen that you need help, for example, in programming. You are allowed to get help from someone who also has an approved access to the project's data — provided that you do NOT leave the screen as long as the help or instructions are ongoing. I.e. if there is a need for a person to help, it must first be ensured that

this person has access to the project. Access can be provided by your institution's FSE-BOA administrators via. FSE-BOA.

That means it is permitted to:

- view and work with microdata on the screen e.g. to check that calculations have gone well
- get help on the screen by someone who also has an approved access to the project's data

What may be transferred from the research machines?

All transferred results must be carried out via the transferring tool. Only by using the transferring tool will it be ensured that the transferred files are scanned for micro data and therefore a warning can be given before the material is transferred, thereby avoiding a possible data breach. A guide to transferring results can be found at our website under "Transferring files"

As a general rule only analytical results, aggregated tables or figures for which it is not possible to identify individual units, i.e. persons, households, families, businesses and other units with de-identified serial numbers, may be transferred. This also applies even if the de-identified serial number has been removed. **In other words, it must not be possible to recognise any individual or company in the material sent**.

In general, the following rules of thumb apply to aggregated data.

As a starting point, transferred results should be of such a form that they can be readily used in a publication

However, further work on the transferred *aggregated* material is allowed, e.g. for the formation of figures or further analysis in statistical programmes, provided that the transferred material meets the above conditions.

For tables, the following applies:

Tables shall contain at least 3 observations per cell

For tables, the rule of thumb is that tables should contain at least 3 observations, but the level of aggregation should always depend on a concrete assessment of what the table contains. If you are in doubt that 3 observations are enough to ensure anonymity, then further aggregates should be made. Aggregation means that cells/numbers are merged until they comply with the number of observations and ensure anonymity.

The requirement applies to the lowest level of aggregation. That is, if you combine multiple variables in a table, then there should be at least three observations in all cells of the variables you combine. If the minimum depreciated is not considered sufficient, then additional aggregates shall be made. The key thing is that aggregation ensures anonymity, and one should also be aware that columns with totals do not reveal any blurred number of observations.

If you work with business data, in addition to the requirement of at least three observations in each cell, you must also comply with the dominance criterion.

For business data, the two largest statistical units (enterprises) together should not exceed 85 % of turnover in a given table cell

Please note that the dominance criterion is always calculated on the basis of turnover, regardless of whether full-time employees and/or another economic variable are reported, e.g. value added in the table. Below is an example of a table where the dominance criterion is not met.

If the criteria are not met, then it is necessary to "disclose" data so that the information of individual entities cannot be identified.

This can be done by the following:

1. Aggregation of sub-groups (aggregation).
2. Deletion of dominant values/outliers.

In case of groupings, it is then checked whether the new grouping of units meets both discretionary criteria, i.e. the number criterion (minimum 3 observations) and the dominance criterion. When deleting data, attention should be paid to any need for secondary discretion (also called follow-up discrepancy) so that the deleted data cannot be derived from totals, subtotals or similar.

Example of dominance problem with business data

The table below shows an example of a discretionary problem due to non-compliance with the dominance criterion.

Example of dominance problem

Discretion	Industry	Number of enterprises	Turnover	Turnover of two largest companies — dominance check
No	Main industry	25	DKK 100 million	DKK 70 million
Yes, secondary	Sector 1	5	~~DKK 30 million~~	DKK 20 million
Yes, primary	Sector 2	20	~~DKK 70 million~~	DKK 65 million

The table shows that there are more than 3 establishments in each group, i.e. the table meets the minimum aggregation requirement. As company data are included in the table, it is also necessary to check for dominant companies. This is done by looking at the turnover of the two largest companies in the three groups, see column 5 of the table. For sector 1, the two largest CVR numbers are 67 %. (20/30) of turnover, so there is no dominance problem here. However, for sector 2, the two largest companies account for 93%. (65/70) of turnover, and so we have a problem of dominance. Therefore, the turnover for sector 2 (primary discretion) is first discerned and then the turnover for sector 1 (post-discretionation) is also discounted, otherwise it will be possible to derive the turnover for sector 2.

If the table also included other information — e.g. value added or number of employees in the table above — this information should also be discretionary in sectors 1 and 2 on an equal footing with turnover, as they are economic variables and therefore this information must also meet the dominance criterion.

For the main industry together, the two largest CVR numbers amount to 70%. (70/100) of turnover, so there is no discretion here. Alternatively, to eliminate turnover in the two sectors, one can instead choose to disclose only the turnover of sector 1 and thereby dissociate the turnover for sector 2 and the total for the main sector. However, it must be absolutely certain that the user does not have the

possibility to obtain the turnover of the main industry from other sources, ex. published figures in the StatBank Denmark or previous deliveries.

If one chooses to discrete turnover in the two sectors, then the discretionary table will look as follows:

Example of dominance problem — after discretion

Discretion	Industry	Number of enterprises	Turnover
No	Main industry	25	DKK 100 million
Yes, secondary	Sector 1	5	—
Yes, primary	Sector 2	20	—

Max, median and minimum

Under the microdata schemes it is allowed to transfer values describing a distribution, such as max, minimum and median, often referring to individual individuals. However, it is a prerequisite for transferring these key figures that there is no danger of identification of individuals. Data security must always be given priority and, if there is any doubt about identification when using these values, then they must not be transferred.

Max and minimum and percentiles such as median may only be transferred if there is no danger of individual identification. No person shall therefore be recognisable in the transferred output

Special attention should be paid to whether a material contains outliers, i.e. extreme values and possibly remove them before transferring, e.g. max values. If max and minimum values are to be transferred, observations at both ends of the distribution must be close to each other, so that no observations stand out and thus create a risk of identification.

Figures

Figures may only be transferred if they do not contain identifiable information. In the case of figures, special attention should also be paid to so-called outliers/extreme values.

In addition, it shall be ensured that the figures do not contain embedded microdata, i.e. the observations that form the basis of the figure are also stored in the file. The latter can be ensured, for example, by transferring the figure in pdf format.

In general, figures may only be transferred if they are certain that they do not contain identifiable information. I.e. with Kaplan Meier curves, for example, attention should be paid to small populations and, in the case of scatterplots, special attention should be paid to outliers. That is to say, figures in general may only be transferred if one is absolutely sure that the content cannot identify individual individuals or businesses in any way. If you‘re in doubt, you don’t have to transfer them. Instead, consideration should be given to whether data can be properly transformed to ensure anonymity, e.g. by using average observations based on e.g. 5 observations — if it makes sense.

Especially for educational institutions

It is allowed to transfer information at institutional level. In other words, it is permissible to transfer information aggregated on a single institution number,

provided that the transferred information meets the above requirements, i.e. it is not possible to identify individuals. Please be aware that the aggregation requirement may need to be tightened, as information is taken from an identifiable area. For example, small populations with combined information such as age and gender will increase the risk of transferred information being personally identifiable.

Examples

Two examples of a set of fictitious tables are presented below, where transferring will be prohibited and allowed respectively.

The tables below must not be transferred. The tables do not meet the number criterion, as two of the observations have less than three observations (Herning and Odense). In the lower table an additional variable income is added and here you get further information about the income of the individual from Herning. In fact, this table contains individual information and it must not occur. In other words, these tables are too small to transfer.

Bopæl	Antal personer	
Bornholm	3	
Herning	1	
København	4	
Odense	2	
Aarhus	3	
Hovedtotal	13	
Bopæl	Antal personer	Sum af indkomst
Bornholm	3	1650
Herning	1	750
København	4	150750
Odense	2	400
Aarhus	3	1800
Hovedtotal	13	155350

Below the same two tables, but now with a level of aggregation where they can be transferred without risk of identification and without risk of further information on individuals, as was the case with the person from Herning in the first two tables.

Bopæl	Antal personer	
Bornholm	30	
Herning	10	
København	40	
Odense	20	
Aarhus	30	
Hovedtotal	130	
Bopæl	Antal personer	Sum af indkomst
Bornholm	30	16500
Herning	10	7500
København	40	1507500
Odense	20	4000
Aarhus	30	18000
Hovedtotal	130	1553500

What may NOT be transferred?

No microdata may be transferred from the research machine

Neither via the transferring tool nor by any other means, for example, by writing information from the screen, taking a screen print or an image of the screen with the mobile phone

This also applies to the microdata submitted by the users themselves in connection with a specific project.

Microdata are defined as data containing, for example, the following:

- Data sets — or parts of data sets — with information at individual/enterprise level — i.e. data linked to a single individual or enterprise. This also applies in cases where the de-identified ID variable has been removed — e.g. the personal identification number or the CVR number. I.e. an individual-level data set consisting of background information such as income, education and socio-economic status or calculated variables at individual level, but where the pseudonymised personal identification number for each person has been removed. The same applies to companies
- Pseudonymised key variables such as personal identification numbers, CVR numbers, workplace numbers, address codes, etc. are always considered as microdata as they indicate a unique number that refers directly to a single person or company. Pseudonymised personal identification numbers etc. may never be transferred whether or not they are linked to other information;

Be aware of application files and logs

Applications and logs may also contain microdata such as:

- Program code that contains microdata written into a condition
- Logs that list observations. Some procedures, for example, list a small sample of the data set used for the analysis

A transfer log that lists pseudonymised PINs is always considered a rule breach — even if these PINs do not contain any other information.

All work with microdata must be carried out on the research machines;

It is allowed to form logs that list pseudonymised personal numbers — e.g. as control of a program, but such a file SHALL, like any other files containing microdata, stay on the research machine and may NOT be transferred.

The users' own microdata submitted to Statistics Denmark to participate in a project are subject to the same rules. That is to say, it is not allowed to transfer your own microdata from the research machines either.

Tables with less than three observations shall not be transferred

If the tables contain fewer than three observations, these tables shall be further aggregated, e.g. by adding categories, or alternatively blinding cells with few observations before the table is transferred. Blinding can be done, for example, by deleting the cell's contents or replacing it with a marking such as"'. If you blind cells, you should be aware that it must not be possible to count back and find the value that has been blinded — for example, if only one cell is blinded and the total is indicated, then at least two cells should be blinded. It is therefore best to merge categories, if possible, in order to avoid this problem.

In addition, for business statistics one additional confidentiality rule applies to economic variables (e.g. turnover or value added), the so-called dominance criterion. This means that if the largest or the two largest companies in a table cell together represent a dominant share, i.e. 85 % of the value in the cell or more, then the dominance criterion comes into force and the cell should be blinded, see the example on page 5: Example of dominance problem with business data.

Especially around the institution register

The institution register shall not be allowed to transfer information at institution level other than the institution number. This means that the associated pseudonymised address codes and CVR numbers may not be transferred to the institutions. We consider this to be transferring of microdata, even if the same information is publicly available.

Examples of microdata

Below are examples of microdata to remain on the research machine.

Table 1 shows an example of data containing microdata. The table provides information on the sex, income, residence, age and a reference to the children of 12 persons. This information refers directly to an individual and may not be transferred.

Table 1. Example of microdata

PNR	KØN	INDKOMST	BOPÆL	ALDER	PNRB
1	M	1500000	København	40	15
2	M	1500	Aarhus	45	22
3	K	1000	Bornholm	50	37
4	M	500	Bornholm	50	65
4	M	250	København	40	87
5	M	150	Aarhus	20	
6	K	150	Odense	25	
7	M	750	Herning	35	19
8	K	500	København	60	74
9	M	250	Odense	65	74
10	K	150	Aarhus	20	
11	K	50	Bornholm	15	
12	M	0	København	10	

In Table 2, the identification variables pnr and pnrb have been removed. However, it is still microdata because the information can be attributed to a single individual. They must therefore stay on the research machine as well.

Table 2. Example of microdata

KØN	INDKOMST	BOPÆL	ALDER
M	1500000	København	40
M	1500	Aarhus	45
K	1000	Bornholm	50
M	500	Bornholm	50
M	250	København	40
M	150	Aarhus	20
K	150	Odense	25
M	750	Herning	35
K	500	København	60
M	250	Odense	65
K	150	Aarhus	20
K	50	Bornholm	15
M	0	København	10

In Table 3, the file from Table 1 contains only the pseudonymised personal identification number. Pseudonymised personal identification numbers are always microdata and may not be transferred. It is irrelevant that all the other variables have been removed. This is still individual data, as the information can be attributed to a single individual.

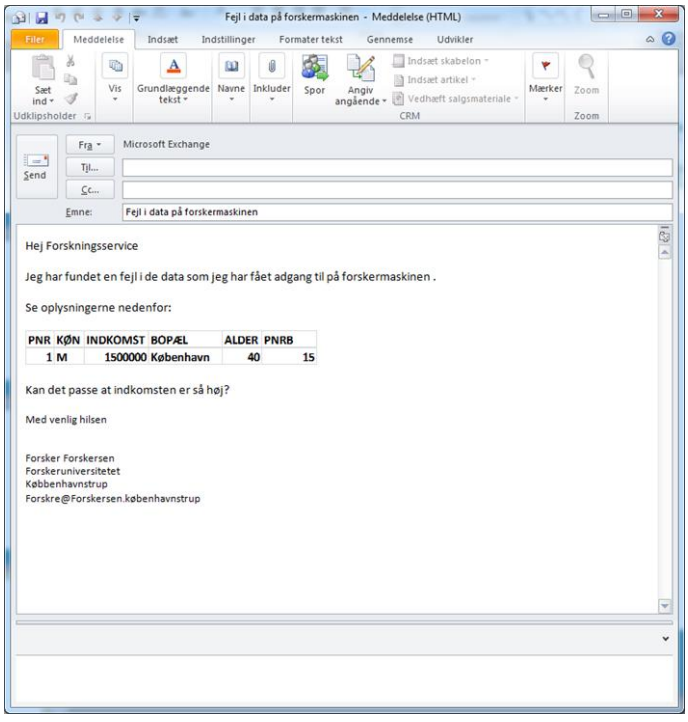
Table 3. Example of microdata

PNR
1
2
3
4
4
5
6
7
8
9
10
11
12

All microdata, whatever form, must remain on the research machine.

It is also not allowed to transfer microdata by email — e.g. in connection with troubleshooting. This applies even if the file is sent to an employee in Research Service or an employee in a specialised office.

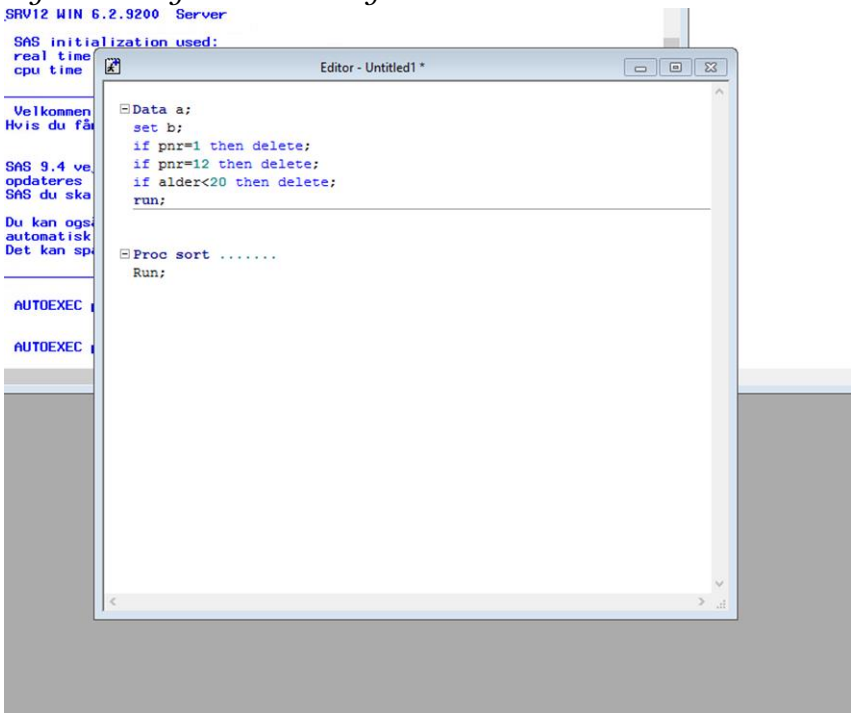
Figure 1. Microdata on mail



If you find an error in the data you have been provided or have some specific questions about microdata that you would like to show an example of, then you have to form a file and save it on the research machine. Then you need to inform FSE about where the file is located — typically refer to the path where the file is located. Then FSE can access the research machine and view the file. This ensures that these files remain on the research machine.

Care should also be taken to transfer programmes from the research machine, as they may also contain microdata, see the example below:

Figure 2. Program containing microdata.



The program encoded pseudonymised personal numbers directly into the program. If such a program is transferred, then it is a breach of the rules of transferring. Therefore, be careful to program such information directly into the program. Instead, use some general rules to remove outliers in a data set, e.g. if the income is higher or equal to 1500000 etc. see Table 1. To avoid encoding personal data directly into the program.

Microdata can be included in programmes, but then they have to stay on the research machine, and you expose yourself and the authorised institution to an increased risk of data breaches. For example, it could be if the program is later taken over by another user and transferred.

Procedures and sanctions in breach of data confidentiality

If a breach of data confidentiality is detected, a distinction is made between transferring of detailed tables and transferring of microdata.

If we find that microdata have been transferred, we will close the access of the institution and follow the procedure described below.

If we find that tables with less than three observations have been transferred in the cells, we do NOT close access, but contact the user for a statement and guide the user on the rules for transfer of data. In the case of repeated breaches of the discretion requirement or if the level of detail in the transferred tables is very high (e.g. if the

vast majority of cells contain 1 digits), then the case may be treated as transferring of microdata.

Sanctions apply to both the individual user and the authorised institution owning a project

The core of the microdata schemes is that Statistics Denmark authorises specific institutions to use data for specific analysis projects. It is important that we can have full confidence in the institutions that we authorise. Statistics Denmark has a good knowledge of the authorised institutions, while the knowledge of the individual users is much better in the authorised institutions than at Statistics Denmark. That is why it is crucial that we can rely on the institutions to give 100 % credit to the users they want to give access to their projects. The institutions must guarantee that the users working on their projects have the necessary competences and that they are well aware of the rules on data confidentiality, transferring, etc.

Each authorised institution has therefore appointed a responsible manager who is responsible for — and oversees — that users associated with their projects are aware of Statistics Denmark's data confidentiality rules and guidelines for transferring.

The agreements made between Statistics Denmark and the authorised institutions and their users state, among other things, that a serious breach of the data confidentiality rules will mean that users who infringe the rules can be excluded from using Statistics Denmark's microdata schemes permanently or for a period of time. Similarly, the institution that owns the specific project may be excluded from the use of the schemes. A breach of the data confidentiality rules can therefore have consequences both for the person who break the data confidentiality rules and for the remaining projects and users linked to the authorised institution in question, which owns the project in question. The reason for this is that a serious breach of data confidentiality rules suggests that the authorised institution involved has not taken its responsibilities sufficiently seriously. This is a problem for the whole microdata scheme. Therefore, the penalty is directed not only at the individual user, but also at the authorised institution, which is responsible for ensuring that the user in question knows the rules and complies with the rules.

Transferring detailed tables

In case of transferring of tables where we consider that there is a risk of identification of individuals, the user who has transferred the file and the authorisation officer of the institution where the user is affiliated, will be contacted and asked to send an account of the transfered and confirm that the file has been deleted. Similarly, an explanation will be requested of how infringements will be avoided in the future. In the case of individual breaches, this will normally not have consequences for the user and institution for access to microdata, but in the case of repeated breaches of rules where tables have been transferred where there is a risk of identification of individuals, this practice may lead to the closure of the institution's access to microdata and further processing of the case similar to the transferring of microdata.

Transferring of microdata

If Statistics Denmark finds that a user has transferred microdata, the user's access to microdata and all projects belonging to the authorised institution that owns the project from which the microdata has been transferred, shall be immediately closed. If a user transfer microdata on a project that is not owned by their own institution, but by another authorised institution, the institution that owns the project is closed — not the user's own institution. The data security responsibility of a user is always the

responsibility of the project-owning institution. For the user who has transferred microdata, access to all projects is closed regardless of which institution they belong to.

Then, the user who has transferred the file and the person responsible for the authorisation agreement of the institution will be contacted. They are prompted to immediately delete all files that violate microdata transfer rules and send a confirmation that all files that violate the rules have been deleted. This applies both to data located on hard drives, mail accounts and where this data may otherwise be stored.

In addition, Statistics Denmark will ask for a description of the breach of the rule, as well as the extent of transferred files that violate the rules. The responsibility for drawing up the report lies with the authorising officer of the institution. Subsequently, Statistics Denmark will ask the institution to send a plan as soon as possible on how it will avoid further breaches of rules in the future. All accesses will remain closed until both the statement and the plan are received.

The Executive Board of Statistics Denmark then decides on the penalty to be imposed on the institution.

As a starting point, the penalty will be to close off access to microdata for all users and projects linked to the institution for at least one month, as well as for the user concerned all access to microdata during the same period. In the event of repeated breaches, access will be closed for a longer period of time or, in particularly serious cases, permanently. If you've committed a breach, there's a waiting period of two years. In other words, if you commit a new break within two years, the penalty will increase, corresponding to the table below. For example, a new break within the waiting period could result in the institution being closed for two months. After two years, a breach is time-barred and it will no longer be taken into account in subsequent penalties.

If the user informs Statistics Denmark that they have transferred microdata, it will be considered as a mitigating circumstance, and this will make it possible for the data access to be opened again as soon as Statistics Denmark has become aware of the extent and nature of the breach. These breaches are not covered by a waiting period. In other words, these breaches are disregarded when a penalty is imposed if a new breach is discovered by Statistics Denmark.

An indicative summary of sanctions can be found in Table 1.

Table 1. Indicative summary of penalties in case of non-compliance.

		Penalty against institution			Penalty against user	
Transferring of individual data		**1st time by institution**	**2nd time by institution**	**Repeatedly for institution**	**1st time**	**Several times**
a.	Technical accident, without the will to do this	1 month of institution quarantine (may be a mitigating circumstance if, for example, the institution itself notifies the error)	2 months of institution quarantine	3 months of institution quarantine	1 month quarantine from all research projects (may be a mitigating circumstance if, for example, the institution itself notifies the error)	3 months quarantine from all research projects
B.	Conscious action, would look at them (debugging)	2 months of institution quarantine	3 months of institution quarantine	3 months of institution quarantine	2 months quarantine from all research projects	Permanent exclusion
C.	Consciously, attempting to identify	3 months of institution quarantine	3 months of institution quarantine	Permanent exclusion	Permanent exclusion	Cannot occur
Password or access disclosed by authorised person		**1st time by institution**	**2nd time by institution**	**Repeatedly for institution**	**1st time**	**Several times**
a.	Carelessness	1 month of institution quarantine	2 months of institution quarantine	3 months of institution quarantine	1 month quarantine from all research projects	3 months quarantine from all research projects
B.	Intentionally	3 months of institution quarantine	3 months of institution quarantine	Permanent exclusion	3 month quarantine from all research projects	Permanent exclusion

Inform us as soon as possible if data confidentiality is breached

If, by mistake, microdata or detailed tables are transferred, please contact Statistics Denmark as soon as possible.

Inform Statistics Denmark as soon as possible in case of a rule breach

Please describe in the email when data has been transferred and the extent of the transfer. If microdata are transferred, access to microdata will continue to be closed and an explanation and prevention plan must be sent, but it is considered a mitigating circumstance that the institution itself reports the breach of rules.

If a breach of rules is quickly notified, it is considered a mitigating circumstance and may shorten the period during which the institution is closed due to transfer of microdata

As the Board, we do not, in principle, close the institution if we are informed about the transfer of detailed tables, i.e. tables that do not meet the discretionary criteria.

Good advice

Below is a list of good advice on how to avoid breaches of data confidentiality and data security rules:

For the user who has access to microdata:

1. Always check all files that are being transferred
    a. Always contact Research Service in case of doubt
2. Limit the transfer of files to the most necessary.
    a. For example, is it necessary to transfer programs and logs? — they are securely stored under the researcher scheme;
    b. Is it necessary to transfer preliminary results?
3. Check the contents of files by a colleague who also has access to the project before transferring files

For the person responsible for the authorisation:

1. Make a plan to ensure that all users are informed about the rules on data confidentiality and data security under the research scheme
    a. Including that both the last arrival and the foreign user have sufficient knowledge of the rules!
    b. The existence of a contact person in case of doubt in the environment;
2. That all authorised users for whom you are responsible for and have approved attachment agreements are aware of the procedure in case of a breach of rules;
3. That all authorised users are aware of the “traps” that may be working with microdata — e.g. logs may contain microdata;
4. If necessary, make control measures when transferring results
5. If necessary, limit the number of users per project that can transfer the output
6. Regularly check that only relevant users have access to microdata for the institution’s projects;

Examples of infringements

Below are some general examples of different types of data breaks and how to avoid them. The examples are mainly based on the types of data breaches we have seen since 2014, when we tightened our sanctions policy, and the examples will be expanded if we see new types of data breaches.

Type of data breach	Description	How to avoid this?
De-identified PNR sent by email to an FSE employee for troubleshooting	User sends a list of de-identified personal numbers (the PNR variable) by email to their FSE contact person to facilitate the troubleshooting process.	Microdata for debugging shall always be stored on a drive on the research machine. Write to the FSE contact person where on the research machine the file is located. From here, the FSE employee can view the file.
Transfer of microdata-containing programs	A user transfers a large program from the research machine to make sure it is not lost. The transfer system comes with a warning, but the user ignores it and is convinced that it is a false positive warning. Our control of the file shows that the program contains microdata, as the program has encoded personal numbers of outliers to be removed from the dataset.	As a general rule, there is no reason to transfer programmes. They are stored safely on the research machine. They can also be copied from one project to another by an FSE employee if the program is to be used on another project. It is OK to transfer programs from the research machine if you are sure that they do not contain microdata. If you get a warning when transferring a program, it is recommended to get another employee who has access to the project to check the program for microdata.

Type of data breach	Description	How to avoid this?
Transfer of log file with microdata	A user has to view the runs of his program thoroughly and therefore transfers the program's log file. There is a warning that the user chooses to interpret as a false positive warning, as it is only a log file that is transferred.	There are several examples where logs from different programs may contain microdata — e.g. the log file automatically prints a small sample of the file and includes it in the log. It is allowed to transfer Log files, but check them thoroughly before transferring them.
Password lending	A user has forgotten his mobile phone and, incidentally, has a very tight deadline. He therefore borrows login information and mobile number from an employee who also has access to the project.	No matter how busy you are, it is never allowed to borrow anyone else's access to the research machine. The password you get is strictly personal and may not be transferred to anyone else.
Transfer of own submitted microdata	A user has submitted their own dataset with microdata, which must be combined with the other data on the project. As it is the user's own data, the user thinks it is OK that they are transferring the files via the transfer system.	There is no microdata to be transferred from the research scheme. This applies to both data from Statistics Denmark and the data submitted by the users themselves.

Type of data breach	Description	How to avoid this?
Copy results from the screen	A user has formed a table to quickly join a meeting about the project. The user writes down the results from the screen and takes them to the meeting.	It is not permitted to copy results or anything else from the screens that have access to the research machines. All the results you need from the research machine must be transferred via the transfer system.
Take pictures with mobile phone of the screen	A user has some questions for his supervisor and decides to take a picture of the screen with microdata and send the image in a text message to the supervisor to better explain the problem.	It is not allowed to take pictures of the screen with your mobile phone when connected to the research machine. Instead, save the file on the research machine and write to the supervisor where it is located. Then the supervisor can go to the research machine and see the file. This requires that the supervisor has access to the project.
Screen Sharing	Two users do not sit in the same place and want to share a screen so they can both look at a dataset.	Screen parts are not allowed remotely when you have access to the research machines. You can only share a screen if you are in the same room and both have access to the project's data.

Appendix 1 — User Agreement

User Agreement for ***[Name** of User]*

has been made for the establishment of direct electronic access to selected datasets under the microdata schemes:

The following provisions shall apply:

1. The data sets to which access is granted are confidential in accordance with §27 part 3 of the Public Administration Act and §152 of the Criminal Code.
2. Work with microdata under microdata schemes at Statistics Denmark may only be carried out in accordance with the rules of Statistics Denmark. This can be done either by connection from the institution which has been granted authorisation or via a home work place in accordance with guidelines laid down by Statistics Denmark.
3. A PC that is connected to Statistics Denmark must not be left to other people, and the connection must, when leaving the PC, be either shut down completely or "disconnected", i.e. protected from unauthorised use.
4. The passwords provided by Statistics Denmark are personal and may not be lent or communicated to others.
5. Data, as well as derived data sets containing microdata, shall not be transferred directly or indirectly.
6. All returns of results from projects under microdata schemes (tables, analytical results, etc.) may only be carried out in accordance with the guidelines and methods laid down by Statistics Denmark. Statistics Denmark shall log these transfers.
7. No confidential data, including data at individual or company level, shall be transferred — microdata and all outputs shall be aggregated to such an extent that there is no risk of direct or indirect identification of persons or companies. Such identification shall not be attempted.
8. Publications from the project must not contain information that can identify individuals or individual companies.
9. Statistics Denmark can receive publications from the project for information
10. Upon delivery of a physical "token", this must be delivered to Statistics Denmark upon termination of the agreement.

In particular for Project Database Managers:

11. The Project Database Manager is responsible for contact with the Research Service in connection with the institution's projects.
12. The Project Database Manager has access to the project database, but not to the institution's other projects. Excluded are projects where the Project Database Manager is also a user of a project.
13. A recommendation for approval must be submitted for new projects on the basis of the project database.
14. It is the responsibility of the project database manager to extract the database for new and existing projects.
15. For the individual project, extracts may only be formed with content that reflects the agreement reached with the Research Service.
16. The project database cannot contain data from the Pharmaceutical Sales Database unless there is a special approval from the Danish Medicines Agency.
17. No analysis shall be carried out on the project database and no data from the project database shall be transferred or otherwise disclosed.

18. The project database and other project data must be separated by different project numbers and no attempt should be made to link data from different projects.
19. The Research Service transmits data from the project database to the institution's projects.
20. The Project Database Manager shall ensure that all users' access to a project containing a project database under an old scheme has ceased within six (6) months of the conclusion of the agreement.
21. The Research Service must be informed if the Project Database Manager resigns.

Permission to share information in the FSE-BOA user management system

22. I allow the information I have provided below to be shared with other users in FSE-BOA.
    a. For employees in Statistics Denmark I allow to share the information below
        - Name
        - E-mail
        - Contact phone (not mandatory to fill in)
        - Mobile number for SMS token (password)
        - Project Access
        - Connecting agreements
    b. For users affiliated to the same authorised institution, I authorise to share the following information:
        - Name
        - E-mail
        - Contact phone (not mandatory to fill in)
        - Project Access
        - Connecting agreements
    c. I authorise to share the following information with the administrators of other authorised institutions, institutional managers and their deputies:
        - Name
        - E-mail
        - Contact phone (not mandatory to fill in)

    The information is necessary to enable a user with an association agreement to become affiliated to several authorised institutions.

Appendix 2 — Affiliation Agreement

Affiliation agreement between [insert name of user] and [insert name of institution]

1. The responsible person who has signed the authorisation agreement at the authorised Danish institution approves and takes responsibility for the compliance of the associated user **[insert name of the user]** with all applicable rules for dealing with microdata
2. The Danish authorised institution is required to inform the associated user of the rules governing the use of microdata, including the applicable discretionary rules, as well as the rules on the transferring of data.
3. The affiliated user's access to microdata from abroad must go through the Danish authorised institution and passed on in accordance with the rules on home work places.

In particular for foreign users

4. The authorised Danish institution appoints a contact person who ensures all contact between the affiliated user and Statistics Denmark
5. All invoices relating to the affiliated user are sent to and paid by the relevant Danish authorised institution under the invoicing conditions otherwise applicable to the institution;

In particular for company data

6. Persons employed by consultancy firms may not have access to company data. In exceptional circumstances, a derogation may be sought if the project is owned by a public authority or an interest organisation. Contact Research Service regarding exemption.

   Persons employed by other individual companies shall not have access to company data.

A breach of the rules of this agreement will have the effect of excluding users of the institution concerned from using any of Statistics Denmark's microdata schemes for a limited period of time determined by Statistics Denmark — or permanently. The rules for the exclusion of microdata schemes can be found on Statistics Denmark's website under "Hjemtagelse af analyseresultater".