Policy framework of the Action Policy[1]

1 Introduction

Under Section 41 of the Statistics Netherlands Act, the Director General is authorised to decide to grant a department, organisation or institution as referred to in Section 41(2) of the Statistics Netherlands Act access to data.

This allows external organisations to make use of the databases held by CBS in the performance of its statutory duties for the purpose of academic or statistical research.

The datasets made available by CBS contain data about individual persons, households, enterprises and institutions.

CBS will therefore only make these data available provided that appropriate measures have been taken to avoid recognition, security is in place and researchers handle these data with care. In addition, CBS ensures, through contractual agreements, awareness measures and monitoring compliance with the agreements made, that researchers handle these data with care, so that the privacy and information security of citizens and companies remains protected.

CBS verifies whether institutions and researchers are complying with the conditions for protecting personal data and preventing disclosure. In the event of a breach of the conditions, CBS may take action.

Within the context of the principle of legality, it is important for institutions and researchers to be aware of the conditions they must meet and continue to meet. This requires the conditions and conduct to be worded accurately, clearly and unambiguously.

It is also important for institutions and researchers to be aware of the consequences of not complying with those conditions. This policy framework sets out the applicable conditions, those that are monitored for compliance and the consequences of not complying with these conditions.

2. Conditions

Certain steps need to be taken to gain access to microdata. These steps are listed on the CBS website: microdata: conducting your own research .

In summary, institutions need to apply for a so-called Institutional Authorisation, and, once granted, the actual access will be set up via a specific application for a research project. While going through those steps, a number of conditions are assessed and conditions are set under which access to microdata will be allowed. While the conditions mostly apply to the institution, they may in some cases also specifically address researchers.

Sections 41 and 42 of the Statistics Netherlands Act, both the Act itself and the Explanatory Memorandum, provide that conditions can be set regarding access to microdata as well as the terms under which access is granted.

[1] The Dutch version of this Policy is leading

Section 41(2) of the Statistics Netherlands Act, for example, explicitly states that access is only allowed for those organisations and institutions listed in this paragraph.

Section 42 of the Statistics Netherlands Act stipulates that the Director General shall only grant a request as referred to in Section 41 if the Director General considers that the applicant has taken adequate measures to prevent the set of data being used for purposes other than statistical or scientific research.

Both the Explanatory Memorandum to Section 42 of the Statistics Netherlands Act and the Explanatory Memorandum to Section 41 of the Statistics Netherlands Act leave it up to the Director General to decide on the respective conditions.

'The provision of data is subject to a number of restrictions in the first paragraph. First, data may be issued solely for the purposes of statistical and scientific research. Statistical research should particularly be seen as the interpretation of statistics in this regard. Furthermore, CBS can only make data available in respect of which it has taken appropriate measures to prevent the identification of individual persons, enterprises or institutions. Some leeway is left to CBS to determine the level of security of the files, also as it proves not possible to set an exact degree of security by law. The measures set up to prevent the disclosure of individual data may vary per file. By way of a third safeguard, it is provided that provision can only be made to services, organisations and institutions referred to in the second paragraph. Parts (a) through (d) of Paragraph 2 are the main clients of so-called microdata files.'

Also (Explanatory Memorandum to Section 42):

'In specific cases, it is up to the Director General to decide on a request for the provision or use of data. The Director General will ensure that the party making the request will indeed use the data for statistical and scientific research purposes and that they have taken adequate measures to prevent the data being used for other purposes. In this light, the Director General will conclude an agreement with the client, thereby laying down the terms and conditions for the provision, for example, with regard to closing off a secure statistical 'enclave' within a larger organisational context. Among other things, the stipulations to be included in the agreement further cover rules on the exclusive use for statistical or scientific research, the restriction on providing the data to third parties and the restriction on linking the data at an individual level. These stipulations also provide for a presentation to CBS of the draft publication of the research. Experience has shown that the need exists from time to time to adjust the conditions after consultation with users. The Director General is the most appropriate body to assess the conditions that must be met in each individual case to ensure exclusive use for statistical and scientific purposes. In view of the above, this Section therefore does not list the conditions. (Explanatory Memorandum, pages 38 and 39).'

The conditions which CBS imposes on microdata access are laid down in different documents and relate to different phases of obtaining access.

1. Gaining access by applying for an Institutional Authorisation

a) Policy Rule of the Director General of Statistics of 12 July 2021, no. CSB-2021-072, containing the criteria for granting institutions access to microdata of Statistics Netherlands (Institutional Access to CBS Microdata Policy Rule).

b) Application for access to microdata, version 30 July 2021 and any additional information provided by the institution to obtain the Institutional Authorisation.

c) Institutional Authorisation (decision within the meaning of the Dutch General Administrative Law Act).

2. Project agreement and Annexes

Having an Institutional Authorisation is not enough for an institution to perform research. It requires a so-called 'project approval'[2] to gain actual access to microdata. This 'project approval' is given practical form by a project agreement concluded between the parties. The request for a research project with annexes ultimately results in a project agreement with conditions, which are laid down both in the project agreement and in the annexes to the project agreement.

The following documents constitute an integral part of the project agreement:

Annex 1: Research Proposal Microdata Services and the Annexes accompanying it

Annex 2: Publication plan

Annex 3: GDPR ground and purpose

Annex 4: Application From Research 2025 (invulwerkblad)

Annex 5: Cost summary

Annex 6: Rules for using the RA facility (August 2023 version)

Annex 7: Guidelines for RA output (August 2022 version)

The confidentiality agreement and user statement completed and signed in accordance with Article 6(7) of the project agreement.

If applicable, the Application From New Researcher submitted in accordance with Article 3(4) of the project agreement.

The 2025 Catalogue of Services Microdata Services.

[2] Article 2(2) of the Policy Rule refers to 'project approval'. The remainder of this policy framework refers to the project agreement, as this is the name applied by CBS.

3. Output guidelines[3]

a. Guidelines for RA output – August 2022.

b. Providing output or other export files.

c. Publishing policies at institutional level.

Legality

Both the Institutional Authorisation and the project agreement, as well as the Explanatory Memorandum to the Policy Rule, state that CBS verifies whether institutions are complying with the conditions for protecting personal data and preventing disclosure. In the event of a breach of the conditions, CBS may take action. Present document lists the actions CBS takes in case of non-compliance with the conditions set by CBS in relation to microdata access.

3. Enforcement instruments and legal framework

General

The applicant has to follow two procedures to obtain access to microdata. The first procedure involves the application of an Institutional Authorisation, followed by the submission of a project proposal which will result in a project agreement. The project agreement will provide access to microdata in connection to a specific project.

When choosing enforcement instruments, a key issue is to determine the applicable framework. As an example, the instruments under administrative law only serve the enforcement of public-law rules.

Institutional Authorisation - public law

According to the Policy Rule, the decision on an application for an Institutional Authorisation, including a rejection, is a decision within the meaning of the Dutch General Administrative Law Act[4], which may be appealed. A Director General's decision on an objection is subject to an administrative law appeal.

In terms of the deployment of enforcement instruments, CBS will only focus on remedial of the standard rather than punishment, and more concretely in the extreme, suspend or revoke the Institutional Authorisation with the aim of the institution being once again compliant with the conditions imposed by CBS.

Suspending or revoking the Institutional Authorisation

[3] The project agreement makes reference to the Output Guidelines. As output control is an important monitoring phase, these conditions are included separately in this memorandum.
[4] See the Explanatory Memorandum to Article 2 of the Policy Rule.

The decision to revoke or suspend refers to the revocation or suspension of a favourable decision, in this case, the Institutional Authorisation by CBS, by which rights or entitlements were granted to a natural person or legal entity.

Revoking a discretionary decision without an explicit statutory basis is not considered objectionable under national law if there is a sound reason for doing so and the nature of the decision or the law does not preclude it. Similarly, revoking non-discretionary decisions due to incorrect or incomplete disclosure of data in the application is not considered objectionable without an explicit statutory basis. The power to do so implicitly lies in the power to grant or refuse the decision if it involves revocation or suspension as a remedial sanction. As previously indicated, CBS' Action Policy is set up only as a remedial sanction. This means that the period of suspension, for instance, will depend on the time needed for the addressee of the Institutional Authorisation to demonstrate that matters have been put in order. The institution will, for example, have to demonstrate that it has implemented measures to prevent any future violations. This will require a protocol, for example, which will have to be submitted to CBS.

Warning

Before sending a notification of an intention, CBS first suffices with one or more warnings, depending on the seriousness of the violation. The subsequent breach is followed by an intention and the actual decision on (remedial) sanctions. A warning is not a decision, meaning it is not open to appeal.

Intention

A remedial action is preceded by an intention. In its intention, CBS notifies its intent to suspend or revoke the Institutional Authorisation. Such an intention is not a decision (Section 1:3 of the Dutch General Administrative Law Act) that is open to appeal, as it is not a final decision, or not yet, but a draft decision. In essence, the intention serves to provide the alleged violating party the opportunity to present their point of view on the remedial sanction to be imposed, as referred to in Section 4:8 of the Dutch General Administrative Law Act.

Project agreement - private law

The Explanatory Memorandum to Section 42 of the Statistics Netherlands Act shows that it is up to the Director General to decide in a specific case on a request for the disclosure or use of data and that, for this purpose, the Director General will conclude an agreement with the client, thereby laying down the terms and conditions for the provision, for example with regard to closing off a secure statistical 'enclave' within a larger organisational context. Also, the Explanatory Memorandum to Section 41 of the Statistics Netherlands Act refers to an agreement under private law: 'CBS concludes an agreement under private law with a client of a microdata file.' An agreement concluded under private law cannot be enforced by administrative law, as there is no statutory regulation.

This would be different if the 'regulations/conditions' were directly based on Section 42 of the Statistics Netherlands Act. Given the fact that the Explanatory Memorandum refers to 'contracts' and 'agreements under private law', compliance must be enforced using the private law instruments, which derive from contract law.

However, in exercising its powers under private law, CBS must also adhere to the general principles of good governance, also see the mutatis mutandis provision 3:1(2) of the Dutch General Administrative Law Act, and private law standards of reasonableness and fairness will have to be observed.

The instruments under private law that are at CBS' disposal are the following:

Warning

Before making use of the formal legal instruments under private law, CBS will send the party with whom CBS has entered into a project agreement a written warning.

Default notice

A default notice is a written notice in which CBS states that the other party is in breach of the project agreement (giving notice of default). In the default notice, CBS will provide the party in question a second, and often final, opportunity to comply with the agreements, before CBS undertakes another action. The default notice is basically a final warning made by CBS. The default notice is a prerequisite for any subsequent termination of the agreement.

Action for performance

CBS can claim performance of the agreement. This means that the arrangements made must still be complied with. Moreover, compensation may also be claimed for the damages caused by the default. If CBS has an interest in the research, it may also claim performance of the project agreement.

Suspension or termination of the project agreement

Default commences when the other party is given notice of default by CBS for the performance and the other party continues to fail to meet its obligations. In that case, CBS may proceed to terminate the agreement, in which the costs due are to be paid.

In the event of a violation, CBS may, for example, deny researchers access to the microdata, temporarily or otherwise, and deny access with respect to a specific project, temporarily or otherwise, until remedial measures have been put into place. In the event of serious violations, in which the conditions set out in the project agreement can no longer be met, CBS may terminate the agreement and, in cases of very serious violations, it may even revoke the Institutional Authorisation. This layered approach is reflected in the detailed actions to be taken, to be described below.

Concurrence

The Institutional Authorisation has a link with the regulations and restrictions associated with the project agreement. The Institutional Authorisation may be revoked if also those conditions are not being complied with, or action has been or is being taken otherwise contrary to statutory regulations.

Severity of the violation

In addition, the severity of the violation also plays a role in the deployment of the enforcement instruments. The severity of the violation is determined based on the nature of the standard violated and the ensuing possible negative impact on the protection of personal data. CBS distinguishes between minor violations, serious violations and very serious violations.[5]

The following will in any case be considered to constitute a minor violation:

1. Failing to immediately report the loss or theft of:
   a. an RA username and/or password;
   b. a telephone registered with CBS for the RA text messaging code;
   c. an RA token provided by CBS;
2. Lending or keeping unsafe the items listed under 1 a to c; or
3. Failing to communicate changes to the institution in good time, such as name changes, mergers, change of legal personality, or changes relating to the researcher, consider new manager, different type of employment contract, new employer.

The following will in any case be considered to constitute a serious violation:

1. Circumventing the output control by copying, photographing or by any other manner taking over the data aggregated by RA from a screen;
2. Working in a public area;
3. Working on a computer where the Remote Access environment is being accessed via a public, unsecured WIFI network, such as in the train, a restaurant etc.;
4. Allowing an unauthorised person to work in the RA environment;
5. Logging into the RA environment from a country that does not adhere to the GDPR;
6. Breaching CBS' data confidentiality in any other way.

The following will be considered to constitute a very serious violation:
If the use of the Remote Access environment results in a personal data breach. A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. This may occur when:

1. Circumventing the output control by copying, photographing or by any other manner taking over the data aggregated by RA from a screen;
2 Otherwise causing or contributing to a data breach.

Cumulative violations

In qualifying the seriousness of the violation, the number of violations is also relevant. For example, multiple minor violations collectively qualify as a serious violation and multiple serious violations qualify as a very serious violation.

[5] This is at the discretion of CBS. The list below is not exhaustive.

Recidivism

Violations are recorded for a period of three years. If a violation is observed again within this period within the same project or with the same researcher, it will be considered a serious violation, in case of repetition of minor violations, or a very serious violation, in case of repetition of a serious violation. In the latter case, this may result in the Institutional Authorisation being revoked. Also, violations of the project agreement may affect the request for an extension of the Institutional Authorisation.

Culpability

Furthermore, facts and circumstances such as culpability also factor into the deployment of enforcement instruments. In the framework of this Action Policy, deliberate violations are considered to be serious violations.

Incidentally, for every action taken, both the holder of the Institutional Authorisation and the signatory of the project agreement are notified. Ultimate responsibility for compliance with all regulations attached to the Institutional Authorisation and the project agreement is vested in the holder of the Institutional Authorisation.

4. Enforcement of conditions

Supervision is not one of CBS' primary duties. CBS does, however, have a responsibility to ensure that CBS data are handled securely, which is why it is important that CBS monitors compliance with the conditions attached to the Institutional Authorisation and the project agreement.

During the application procedure, the institution was tested on a number of conditions for microdata access based on the Policy Rule, and questions relating to information security need to be filled in. This application forms part of the Institutional Authorisation that has been granted. The questions relate to conditions in terms of information security, for example. CBS expects institutions to have an appropriate level of information security. The Government Information Security Baseline has laid down this security level for government organisations. Research institutions in the healthcare sector are held to the NEN standards for information security in healthcare. As yet, universities and research institutions do not have to comply with statutorily required information security standards, however, they do have to indicate how they have set up their information security and which standards they apply to this end.

There is currently no interim monitoring to check whether institutions continue to meet the conditions for obtaining an Institutional Authorisation. This assessment takes place in the event of an extension of the Institutional Authorisation, which is after the expiry of the one-year or three-year term, or if the institution passes on any changes based on Article 6(5) of the Policy Rule. Given the limited term of the Institutional Authorisation, this is considered to be sufficient. Moreover, according to the conditions imposed on the Institutional Authorisation, CBS must be notified of any changes that are important for the application.

Monitoring is done for the purpose of compliance with the conditions attached to the project agreement. Given that the risks are mainly caused by the human factor, this monitoring focuses

mainly on researchers. The monitoring can be subdivided in active monitoring and monitoring in response to complaints, signals or notifications. Active monitoring pertains to the process of authorisation and identification of researchers, research with regard to the working and labour relationship between the researchers and verifying the IP address in order to establish whether or not logins are attempted from outside the EEA, and the output monitoring.

Complaints, signals or notifications may also prompt CBS to take enforcement action. For example, in response to increased supervision imposed by the Dutch Data Protection Authority (Dutch DPA), CBS may take action with regard to the addressee of the Institutional Authorisation in question, provided the supervision affects the RA environment. In addition, CBS also receives questions about projects showing that the project agreement is being violated.

5. Action Policy

Based on the abovementioned principles, CBS will take the following action towards researchers, the research project or institution in the event of non-compliance with/violation of the regulations/arrangements attached to the Institutional Authorisation or the project agreement.

As previously described, the regulations address the individual researchers, the project as a whole and the holder of the Institutional Authorisation. The regulations pertaining to the researchers are available in the Annexes to the project agreement, particularly the confidentiality agreement and the Rules for the use of the Remote Access facility of CBS, but also in the project agreement itself. It follows that the action to be taken also targets those three norm addressees.

Actions[6] regarding	Action in case of a minor violation	Action in case of a serious violation	Action in case of a very serious violation
Researchers	Suspension of the researchers' authorisation until the awareness test is successfully completed again.	Suspending the researchers' authorisation for three to six months for all projects and successfully completing the awareness test again.	Suspending the researchers' authorisation for at least six months and successfully completing the awareness test again.
Project organisation	Written warning.	Closing off the project environment for a maximum period of six months.	- Suspending the project agreement in full for at least six months or terminating the project agreement. - The organisation has to demonstrate that appropriate measures are in place to prevent recurrence.
Institution	Access to a project or projects are closed off until a reassessment has taken place.[7]	Suspending the Institutional Authorisation.	- The institution has to demonstrate that appropriate measures are in place to prevent recurrence. - Revoking the Institutional Authorisation.

[6] The actions are cumulative in nature. This means: for example, in the case of a serious violation, all actions are imposed in column 3.

[7] This measure is taken only if changes at the institution have not been communicated in time.