Privacy Impact Assessment (PIA)

STATISTICS NETHERLANDS

DIRECTORATE FOR STRATEGY AND EXECUTIVE ADVICE

THE HAGUE, 24 March 2021

Appointment of controller: 24 March 2021
Name: Ms A. Berg

Consultation of Data Protection Officer: 16 March 2021
Name: Mr M. Booleman

Advice CIO: 23 March 2021
Name: Dr A.H. Kroese

Privacy Impact Assessment (PIA)

STATISTICS NETHERLANDS
DIRECTORATE FOR STRATEGY AND EXECUTIVE ADVICE

Contact:

Statistics Netherlands
Mr M. Booleman
Email: M.Booleman@cbs.nl
Telephone number (Infoservice): +31 88 570 70 70

Version: 2.0 23 March 2021

Contents

Introduction

This is the general Privacy Impact Assessment (hereafter: PIA) of Statistics Netherlands (CBS or SN).

Statistics Netherlands (SN) receives a lot of data under the Statistics Netherlands Act [*Wet op het Centraal bureau voor de statistiek*]. Under the GDPR, data source owners or data providers must in some cases draw up a PIA before supplying data to CBS, in order to demonstrate that they are being careful when processing or supplying data. CBS also requires a PIA for processing within its own organisation.

In this context, CBS has drawn up a PIA for use by data providers, which sets out what happens to the data, on what basis, and how the security of the data is safeguarded within CBS.

PIA for regular processes
This PIA is intended as a standard PIA for the regular processes of CBS. A risk analysis is also carried out for each process, in the form of a Baseline Assessment, for example. CBS makes no distinction here between repeating and incidental studies, as data are processed through the same production lines in both cases.
Separate PIAs are drawn up for deviating processes. Among other things, this is the case for innovative processes involving new techniques and methods.

PIA as a basis with additional information in an agreement
In addition to this PIA, a Delivery Agreement is concluded for each administration operator for periodic data deliveries to CBS, in which further information is recorded, such as the purpose of the delivery, the categories of personal data, the time and frequency of deliveries, retention periods, data minimisation, etc. For incidental studies involving the provision of data to CBS, the further information will be recorded in a Project Agreement.

A. Description of data processing characteristics

Describe in a structured manner the intended data processing operations, the processing purposes and the interests in the data processing operations.

Section A describes the first step of the PIA: an overview of the relevant facts of the intended data processing. If the facts are unclear, this will affect the assessment.

1. Proposal

Describe in broad terms the proposal to which the privacy impact assessment relates and the context in which it takes place.

General: CBS is an autonomous administrative authority established by law: the Statistics Netherlands Act (hereafter: 'SN Act'). In the context of statistics, CBS, as the responsible body, processes personal data both automatically and manually.

Task: CBS is tasked by the Dutch central government with conducting statistical research for the purposes of practice, policy and science, and publishing the results of those statistical studies (Section 3 of the SN Act).

Implementation (basis): In order to carry out its task, CBS collects personal data from respondents and businesses (self-employed workers without employees and sole proprietorships) in accordance with Section 33 of the SN Act in combination with Article 6.1(e) of the General Data Protection Regulation (GDPR). These data are used in statistical analyses. The data collected are not retained any longer than is necessary for the statistical tasks of CBS and are therefore destroyed as soon as they are no longer needed for those tasks.

CBS collects data itself, but it also has the right to use, for statistical and scientific purposes, data from registers that are maintained in connection with the performance of a statutory task at:
a. institutions and departments of:
   i. Central government;
   ii. Provinces;
   iii. Local authorities;
   iv. Water boards;
   v. Public bodies established pursuant to the Joint Regulations Act;
   vi.
b. Public bodies as referred to in Section 134 of the Constitution;
c. Autonomous administrative authorities at the level of central government.

CBS will first check whether the data it needs to carry out its task have been included in a register. If this is not the case, CBS itself will conduct surveys of companies and individuals to obtain the data.

Use of the data (purpose limitation): The data received by the Director General of Statistics (DG) in connection with the performance of the duties for the implementation of the SN Act may be used solely for statistical and scientific purposes. Use of the data for taxation, administrative, checking and legal purposes is not permitted (see the memorandum of understanding regarding Section 37(1) of the SN Act). The data are requested for a specific statistic or a group of specific statistics. These are set out in a Supply Agreement in the case of external administration operators in a Project Agreement if data are supplied incidentally.

Access to the data: Access to the data is only possible for those who are responsible for carrying out CBS' task and therefore necessarily need access to the relevant data. CBS is the national statistical institute and it has implemented policies and procedures to ensure that data can be used exclusively for scientific and statistical purposes. These safeguards are included in international regulations (Regulation (EC) No. 223/2009 on European statistics and the European Statistics Code of Practice) as well as national regulations (SN Act). The CBS code of conduct also addresses this matter.

On request, the DG may grant access to a set of data or provide data for statistical and scientific research purposes if appropriate measures have been taken to prevent the identification of individual persons, households and enterprises (Section 41 of the SN Act). Using remote access, the data are analysed by other institutions and results of the research are published at an aggregate level.

Measures include:

1. The DG may only grant institutions or organisational units of institutions access to analysis files if their sole purpose and task is to conduct scientific research;
2. The DG may only approve requests for microdata from a researcher if the researcher's sole purpose and task is to conduct scientific research.

More information about the Remote Access environment can be found on the CBS website. See also the end of point 17 of this PIA.

Confidentiality: the personal data collected is never published by CBS in such a way that those data can be traced back to an identifiable person. Publication is only possible in aggregated form (Section 37(3) of the SN Act). CBS carries out output checks on this.
Deliveries of individual records to third parties are always appropriately secured against identification in accordance with Section 41 of the SN Act. See point 17 of this PIA below.
As civil servants, CBS employees have sworn a solemn oath or made a sworn statement, and they are bound by a duty of confidentiality in accordance with Sections 5 and 9 of the Civil Service Act. To ensure confidentiality, researchers from other institutions are required to sign an agreement and a confidentiality agreement.

Security: As soon as possible after arrival, the personal data are stripped of directly identifying information such as name, address and place of residence. The Citizen Service Number (BSN) is encrypted (pseudonymised). The analyses are only conducted on the pseudonymised files, with less directly identifying characteristics such as date of birth, education number, etc. also being secured.

Assessment: CBS has its information security (ISO 27001), quality (ISO 9001) and privacy protection (NOREA Privacy Control Framework) assessed externally every year. The certificates are placed on the CBS website. https://www.cbs.nl/nl-nl/over-ons/organisatie/privacy/iso-en-privacycertificering

2. Personal data

List all the categories of personal data that are processed. For each category of personal data, indicate to whom it relates. Classify these personal data into the following types: ordinary, special, crime-related and legally identifying.

CBS may receive and further process both special and non-special personal data for its statistical tasks, provided the requirements under the relevant legislation and regulations referred to are observed. See also CBS Bronnen.

Diversity of data: CBS receives various personal data in accordance with the Statistics Netherlands Act (SN Act). These include data relating to gender, age, marital status, income, health, welfare, education, pensions and youth care, and subjective assessment questions about the home, living situation and safety. But data on income support and unemployment can also be involved. For sole proprietorships and self-employed workers without employees, this could include data on production, revenues, etc.

Citizen Service Number (BSN): The DG may include the Citizen Service Number in a register and use it for statistical purposes. The BSN may be used in contacts with persons and institutions, insofar as these are themselves authorised to use that number in a register (Section 34 of the SN Act).

Special data:
CBS may process special categories of personal data for statistical purposes under Section 35 of the SN Act (Article 9 of the GDPR in conjunction with Paragraph 3.1 of the Dutch GDPR Implementation Act [*Uitvoeringswet AVG*]), such as race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data, health, and sexual behaviour or sexual orientation. On the basis of Section 9(2), opening words and (j), and Section 24 of the Dutch GDPR Implementation Act, the data may be processed if the processing is necessary for scientific research or statistical purposes in accordance with Article 89(1) of the GDPR and the other conditions of Section 24 of the Dutch GDPR Implementation Act have been met. See point 12 of this PIA below.

Crime-related data:
CBS may also process personal data of a criminal nature for statistical purposes under Section 35 of the SN Act (Article 10 of the GDPR in conjunction with Paragraph 3.2 of the Dutch GDPR Implementation Act). Under Article 10 of the GDPR and Section 32(f) and Section 24 of the Dutch GDPR Implementation Act, the data may be processed if the processing is necessary for scientific research or statistical purposes in accordance with Article 89(1) of the GDPR and the other conditions of Section 24 of the Dutch GDPR Implementation Act have been met. See point 12 of this PIA below.

3. Data processing operations

List all intended data processing operations.

Data collection is followed by a technical check, pseudonymisation, linking and classification, checks and corrections (editing), aggregation and tabulation, analysis and publication, and finally, storage https://www.cbs.nl/nl-nl/over-ons/organisatie/statistisch-proces

These processing operations are recorded in the Register van de verwerkingsactiviteiten.
In addition, CBS has an extensive source list and an overview of more incidental processing operations:

- Uitgebreid overzicht van bronnen van het CBS
- Overzicht meer incidentele verwerkingen

4. Processing purposes

Describe the purposes of the intended data processing operations.

CBS is tasked by the Dutch central government with conducting statistical research for the purposes of practice, policy and science, and publishing the results of those statistical studies (Section 3 of the SN Act). It is also responsible for implementing statistical European regulations (Section 4 of the SN Act). CBS therefore processes data for statistical and scientific purposes, to improve the quality of statistics and to develop new statistical information. CBS may also perform statistical work for third parties on an occasional basis (Section 5 of the SN Act).

5. Parties involved

List which organisations are involved in which data processing operations. Classify these organisations for each data processing operation under the roles: controller, processor, provider and recipient. Also specify which officials within these organisations have access to which personal data.

CBS meets the very highest standards in relation to data protection. Privacy protection is reviewed annually in a Privacy Audit Framework. Privacy protection encompasses all the measures that ensure the proper protection of personal and company data. A large proportion of these measures relate to securing the data and therefore overlap with the requirements for information security. Privacy audits therefore also deal with aspects of information security according to the NOREA framework. NOREA is the professional organisation for IT auditors (for more information on information security, see point 17 on measures). Privacy audits have been carried out at CBS since 2015. They are carried out by an external auditor and result in a privacy-proof verklaring.

Together with the ISO27001 certification, the legal accountability of the data supplier is thus fulfilled. This also means that the data supplier's responsibility ends once the files have been received by CBS. CBS is the controller. Furthermore, in a number of cases, certain CBS tasks are outsourced to third parties (processors).

CBS is the controller
Under Section 3 of the SN Act, CBS has the task of compiling statistics for the benefit of policy, practice and science. In accordance with Section 18 of the SN Act, the Director General of CBS also determines the methods used to conduct statistical studies and the manner in which the results of these studies are to be published. CBS is independent in this regard; it cannot and may not take instructions in this from others. The controller (Article 4(7) of the GDPR) is the body that determines the purposes and means of processing personal data. On the basis of these two legal provisions, CBS is always the controller and never a processor.

Processors
CBS sometimes outsources a number of tasks, for which it uses processors. These processors are included in the internal register of processors. They include fieldwork agencies that receive name and address details in order to carry out face-to-face observations in households. The survey results are then sent to CBS in a secure manner. A processor's agreement is always concluded with processors.
In the event of collaboration, a collaboration agreement will set out which external parties will be hired, what their activities will be and which data this party will receive.

Recipients
Data may be appropriately protected (see point 17 of this PIA below) and provided on request to the following parties in accordance with the SN Act:
1) CBS employees charged with carrying out the statutory task of CBS (Section 37(2));
2) Community and national statistical authorities of the member states of the European Union and the members of the European System of Central Banks, insofar as such provision is necessary in accordance with a decision of the European Council and the European Parliament (Section 39);
3) De Nederlandsche Bank (DNB) in the context of the implementation of the External Financial Relations Act 1994 [*Wet financiële betrekkingen buitenland 1994*] (Section 40);
4) for the purpose of supplying statistical or scientific research to a department, organisation or institution. This could be (Section 41):

a. a university within the meaning of the Higher Education and Scientific Research Act [*Wet op het hoger onderwijs en wetenschappelijk onderzoek*];
b. an organisation or institution for scientific research established by law;
c. planning offices established under or pursuant to the law;
d. the Community statistical agency and national statistical agencies of the member states of the European Union;
e. research departments of ministries and other departments, organisations and institutions.

6. Interests in relation to data processing

Describe any interests that the controller and others have in the intended data processing operations.

CBS itself has no interest in the results of the research other than that the research is done in a proper manner as regards quality. The intended processing is always necessary for CBS to carry out its tasks.

7. Processing sites

List the countries in which the intended data processing will take place.

The processing location is CBS in the Netherlands (The Hague, Heerlen).
The computer centre is located in Almere.

In addition to its responsibility for European Dutch statistics, CBS is also responsible under Sections 4 and 32a of the SN Act for producing European (Community) statistics and statistics for the Caribbean Netherlands (Bonaire, St Eustatius and Saba).
The CBS office on Bonaire is the central point for the collection of data and the publication of statistics. The statistical information is analysed and processed at the CBS offices in The Hague and Heerlen. In the statistical process, there is no transfer of personal data from CBS in the Netherlands to Bonaire. The information published by CBS is about subjects that affect the people of the Caribbean Netherlands. These include economic growth and consumer prices, the income situation of individuals and households, but also health and leisure.
Personal data are provided to CBS by organisations from the Caribbean Netherlands in accordance with the Personal Data Protection Act BES [*Wet bescherming persoonsgegevens BES*].

8. Technology and method of data processing

Describe how and with what technical and other means and methods personal data are processed. State whether there is any automated or semi-automated decision-making, profiling or big data processing and, if so, give details.

CBS only processes data for scientific research or statistical purposes. There is no automated or semi-automated decision-making or profiling.
When published, the data can never be traced back to one person or to a very homogeneous group of people (e.g., 'nearly all the people in this neighbourhood are below the poverty line').

In general terms, the following security measures are taken: shielding of production data from the Internet and scanning of all data from and to the production environment;
secure workstations; shielding from the use of data carriers; access control and securing buildings; pseudonymisation of identifying data; testing of security measures by means of internal and external audits and tests. See point 17 of this PIA below.

9. Legal and policy framework

List the laws and regulations – other than the GDPR and the Directive – and policies with potential implications for data processing.

The Statistics Netherlands Act, the Statistical Law (European Regulation 223/2009), the European Statistics Code of Practice and the CBS Code of Conduct.

CBS may receive data under Section 33 of the SN Act. Section 33(4) of the Act states: *"At the request of the Director General, the institutions, departments, bodies and independent government bodies referred to in Section 33(1), the legal entities referred to in Section 33(2) and the companies, independent professionals, institutions and legal entities referred to in Section 33(3) shall provide the data referred to in Section 33(1-3) free of charge within a period to be stipulated by order in council. In such cases no duty of confidentiality may be invoked, unless this duty is based on international regulations."*

For data processing by CBS, which is responsible for producing Community statistics at national level, CBS' work programme is important:

The main lines of the work programme are laid down in a Multi-annual Programme (Section 14 of the SN Act). A work programme is adopted each year by the DG (Section 15 of the SN Act). The work programme also includes the Community statistics that CBS is required to compile under Section 4 of the SN Act. The data processing is therefore necessary for the performance of a task of general interest.

10. Retention periods

Determine and justify the retention periods of personal data based on the processing purposes.

In the context of retention periods, CBS distinguishes between personal data in the 'input base' and the 'microbase', and personal data in 'intermediate files'.

Input base
The input base contains the personal data (possibly encrypted) as received by CBS. These are the incoming (raw) personal data files. These personal data are pseudonymised/encrypted as soon as possible after receipt.
For personal data used for monthly, quarterly and annual statistics, a maximum retention period of 2.5 years applies after the end of the reporting year to which the data relate. For personal data used for a statistic with a periodicity of 2 or more years, the retention period equals the periodicity plus 1 year after the end of the reporting year to which the data relate.
This enables CBS to go 'back to the source' where necessary. There is no reason to keep these files for longer than mentioned above, because the data used to produce statistics are stored in the microbase.

Microbase
The microbase contains the pseudonymised files from the input base after they have been further processed and prepared for compiling statistics. The files in the microbase directly underlie the statistical process.
Personal data in the microbase are retained for a long period of time, with the justification for retention being reviewed every 3 years. The non-personal data in the microbase are stored permanently.
The main reasons for data retention or for longer retention are as follows:

- In the case of changes to the source, method or process, it is often desirable to repair breaks in time series that result. The best way to do this is to reprocess microdata that have been used in the past. This is often a reason to keep files.
- For longitudinal research, it is regularly necessary to reaggregate old data to produce tables that are comparable to newly produced tables.
- Some CBS datasets, such as the censuses, may be regarded as historical heritage. According to the Public Records Act, CBS has the obligation to keep data and related publications in good, orderly and accessible condition.
- The microdata in the microbase are made available to scientists, among others. The legal frameworks for this are laid down in Sections 39 to 42 of the SN Act. It is not possible to predict what questions these scientists will have, which makes it impractical to compile aggregates relevant to this use. The fact that microdata can be drawn on and data are available for increasingly long periods of time makes this facility even more relevant. This also applies to the use and reuse of microdata by CBS itself. There is a retention period of 10 years for data used for PhD research.

Intermediate files
As part of processing for statistical purposes, various 'intermediate files' are usually created from microbase files.
Intermediate files are kept for as long as is necessary for the ongoing process. This means that they are deleted after completion of a statistical study.

Finally, the retention period for backup files is three weeks. This period is stated in the memorandum 'Revision of Backup Policy' of 30 March 2011.

B. Assessing the lawfulness of data processing

Assess whether the intended data processing operations are lawful on the basis of the facts as set out in Section A. This concerns the assessment of the legal ground, necessity and purpose limitation of the data processing operations. In addition, assess the way in which the rights of data subjects are interpreted. Legal expertise is needed in particular for this section of the PIA.

11. Legal ground

Determine the legal grounds on which the data processing operations will be based.

The statutory task and legal obligations form the legal grounds for processing personal data as stated in the SN Act (Sections 3, 4 and 5 of the SN Act).

12. Special personal data

If special or crime-related personal data are processed, assess whether one of the legal exceptions to the processing prohibition applies. For the processing of a legal identification number, assess whether it is permitted.

See question 2.

CBS processes special personal data as referred to in Article 9 of the GDPR for statistical purposes. The basis for processing these special personal data is Article 9(1)(j) of the GDPR and Article 89 of the GDPR in combination with Section 35 of the SN Act.

Section 35 of the SN Act is in line with Section 24 of the Dutch GDPR Implementation Act. This section indicates that the ban on processing personal data as referred to in Article 9 for the purpose of scientific research or statistics does not apply, insofar as:

- processing is necessary for scientific or historical research or statistical purposes in accordance with Article 89(1) of the GDPR;
- the research referred to in point 1 serves a general interest;
- asking for explicit consent proves impossible or involves a disproportionate effort; and
- the implementation is provided with such safeguards that the privacy of the data subjects is not disproportionately impaired.

Furthermore, CBS processes personal data as referred to in Article 10 of the GDPR, also for statistical purposes. Data of a criminal nature may be processed on the basis of Article 10 of the GDPR in conjunction with Section 32(f) of the Dutch GDPR Implementation Act in conjunction with Article 89 of the GDPR. The processing is necessary for scientific or historical research or statistical purposes in accordance with Article 89(1) of the GDPR, and the conditions referred to in Section 24(b to d) of the Dutch GDPR Implementation Act (Section 32 of the Dutch GDPR Implementation Act) are met.

Section 24 of the Dutch GDPR Implementation Act

Section 24 of the Dutch GDPR Implementation Act imposes the following conditions:

a. processing is necessary for scientific or historical research or statistical purposes in accordance with Article 89(1) of the GDPR;

   In accordance with its statutory task, CBS only processes data for scientific research or statistical purposes. CBS has taken additional procedural and security measures to limit the use of special personal data to a minimum, such as additional mandatory and explicit approval. This means that there is passive consent for confidential data and active consent for special and crime-related data. Each file has an owner, who gives permission for its use.
   As a standard part of the process, it is considered whether the purpose can be achieved by processing less or no personal data within the meaning of the GDPR. The purpose of the processing is also assessed.
   In addition, as soon as possible after receipt of the personal data, they are stripped of directly identifying information such as name, address and place of residence. The Citizen Service Number (BSN) is encrypted (pseudonymised). The analyses are only carried out on the pseudonymised files.

b. the research referred to in point a. serves a general interest;

   The Explanatory Memorandum to the SN Act (House of Representatives, 2001-2002 session, 28 277, no. 3, explanatory notes to Section 35, p. 35) states: "In general it can be said that CBS serves a substantial public interest in performing its task." It is also stated that the SN Act contains sufficient appropriate safeguards to protect the privacy of natural persons. Reference is made here to Section 37 of the SN Act in relation to the use of data and publication. This provision rules out the publication of personal data by CBS.

c. asking for explicit consent proves impossible or involves a disproportionate effort; and CBS uses various registers and surveys as sources. The SN Act states that CBS has the right and the duty to use data from these registers for statistical and scientific purposes (Section 33 of the SN Act). In view of the above and the number of data subjects from whom CBS has to process personal data for the performance of its statutory task, it would take a disproportionate effort to ask the data subjects for their explicit consent.

d. the implementation is provided with such safeguards that the privacy of the data subject is not disproportionately impaired.

CBS complies with this by taking technical, organisational and legal measures, such as appropriate security (see points 8 and 17), data minimisation and a legal ban on the publication of personal data.

13. Purpose limitation

If personal data are processed for a purpose other than that for which they were originally collected, assess whether such further processing is compatible with the purpose for which the personal data were originally collected.

The data may only be processed for statistical or scientific research purposes.
Use of the data for taxation, administrative, checking and legal purposes is not permitted (Section 37(1) of the SN Act).
Extended purposes are considered to be all processing operations aimed at improving the quality of statistics as well as research on the design of new statistics or new statistical processes.
See also point 1 of this PIA.

14. Necessity and proportionality

Assess whether the intended data processing operations are necessary for achieving the processing purposes. In doing so, address at least the questions of proportionality and subsidiarity.

a. Proportionality: are the invasion of privacy and protection of personal data of the data subjects proportionate to the purposes of processing?

b. Subsidiarity: can the processing purposes not reasonably be achieved in another way that is less detrimental to the data subject?

The data CBS receives are necessary for performing the statutory task assigned to CBS. Without the data, CBS cannot fulfil its statutory task.
Because data can never be traced back to an individual when published, individuals are never directly or indirectly affected as a consequence of the processing.
The request for data and the processing of those data always involve data minimisation within the meaning of the GDPR. For example, the supply agreement sets out the specific purpose or purposes for which the data are needed.
It is standard in the process to weigh up and assess whether the purpose (the statistic in question or the planned research) can be achieved by processing fewer or no personal data.
When special or crime-related personal data are involved, it is also considered and assessed whether the same result can be achieved with ordinary personal data or a combination of ordinary personal data.

15. Rights of the data subject

Indicate how the rights of data subjects are implemented. If the data subject's rights are restricted, identify which legal exceptions allow this.

Section 44 of the Dutch GDPR Implementation Act makes an exception for scientific research and statistics. Where processing is carried out by institutions or departments for scientific research or statistics, and the necessary provisions have been made to ensure that the personal data may be used solely for statistical or scientific purposes, the controller may disregard Articles 15 (right of access by the data subject), 16 (right to rectification), 18 (right to restriction of processing) and 21 (right to object) of the GDPR.

Data subjects from whom CBS receives data via register holders are not directly informed by CBS about the data processing on the basis of the exception in Article 14 (5)(b) of the GDPR. The reason for this is that CBS uses various registers and surveys as sources, and the SN Act stipulates that CBS has the right (and the duty) to use data from these registers for statistical and scientific purposes (Section 33 of the SN Act). Informing these indirect data subjects would then require a disproportionate effort.

However, having regard to Article 14(5)(b) of the GDPR, CBS is obliged to publish information about its processing activities and CBS complies with this obligation by maintaining a register of sources and by publishing information on the statistical process on its website. In addition, when statistical information is published, the sources that led to this information are included.

When carrying out surveys, CBS actively informs the data subject by means of an information letter accompanying the survey. Reference is also made to the CBS website, the study design and the sources used, and a help desk is available for questions about the study.

The website contains a privacy statement and an explanation of the right of access.

C. Description and assessment of risks to data subjects

Describe and assess the risks of the intended data processing operations to the rights and freedoms of data subjects. In doing so, take into account the nature, scope, context and purposes of the data

processing as described and assessed in Sections A and B. This does not concern the risks to the controller.

16. Risks

Describe and assess the risks of the intended data processing operations to the rights and freedoms of data subjects. In doing so, address at least:

a. what adverse consequences the data processing operations may have for the rights and freedoms of data subjects;
b. the origin of these consequences;
c. the likelihood (probability) that these consequences will arise;
d. the severity (impact) of these consequences for the data subjects when they arise.

Re a.
The processing operations serve exclusively statistical purposes and therefore do not adversely affect the rights and freedoms of data subjects, since the purpose is always to produce aggregated data from which no data relating to individuals can be derived. There is only the risk of a data leak, which is a potentially high risk.
Re b. Employees who may have access to the data, or external causes of a data leak.
Re c and re d. After taking the necessary measures, an acceptable residual risk remains.

CBS has access to high-risk information, both in terms of the breadth (many sensitive and non-sensitive data) and depth (many individuals), so that the privacy impact in the event of a data leak can be high. However, in view of the potentially high risk, appropriate technical and organisational security measures have been taken in accordance with ISO 27001. Furthermore, all CBS processing operations are designed to minimise the risk of individuals being identified or traced. This minimises the risk to the data subject.

D. Description of planned measures

Section D considers what measures can be taken to prevent or reduce the risks recognised in Section C. The choice of measures to be reasonably taken involves a balancing of interests by the legislator or the controller. For this part of the PIA, expertise on information security is important when it comes to security measures.

17. Measures

Assess what technical, organisational and legal measures can reasonably be taken to prevent or reduce the risks described above. Describe which measure addresses which risk and what the residual risk is after implementation of the measure. If the measure does not fully cover the risk, justify why the residual risk is acceptable.

Based on the 2015 CBS-wide risk analysis, the conclusion is that CBS' confidentiality level is 'Restricted' (Dep.V.), based on the criteria listed in the 2013 Civil Service Information Security (Classified Information) Decree (VIRBI). The processing of special personal data also falls under risk class 2 of the Dutch Data Protection Authority.

CBS uses the ISO 27001/2 standard and the Government Information Security Baseline (BIO) as a basis for determining the necessary measures. The risks are sufficiently covered by the measures taken. Complete coverage of the risks will never be possible because the human factor, often the most important factor in a security incident, can never be completely excluded.

The scope encompasses all primary and all supporting processes of Statistics Netherlands, and the information systems used for those processes, where information system is understood to mean: the coherent whole of data collections and the persons, procedures, processes and software associated with them, as well as the storage, processing and communication facilities established for the information system.

Security procedures are the direct responsibility of line management. CBS periodically checks compliance with the reliability measures:

- A report is drawn up every quarter containing notifications relating to privacy and security.
- An external IT security audit is conducted every two years.

The ISO-27001 certification of the information security management system used. The certificate is on the CBS website.

Monthly penetration tests (vulnerability scan) are performed on the web servers. More in-depth (black box) penetration tests are also performed.

CBS has laid down the security measures in the process documentation and these are correct, complete and up to date.

With regard to the staff:

- all CBS employees and interns have signed a confidentiality agreement in which the obligations and responsibilities relating to confidentiality are laid down;
- CBS employees are civil servants and they are therefore bound to treat as confidential all information that comes to their knowledge through their work. In addition, they have sworn a solemn oath or made a sworn statement and signed a declaration containing the oath or statement;
- temporary external staff, agency staff and interns also sign a confidentiality agreement, but do not swear an oath or make a sworn statement as they are not appointed as civil servants;
- confidentiality agreements are required of third parties;
- where appropriate, confidentiality will be laid down in agreements with third organisations (such as scientific institutions) that are granted access to personal data;

Logging is carried out by the IT department of CBS at the user level. There is also logging in the intrusion detection system. Logging takes place in the central IT systems as well as the decentralised IT systems.

The manner in which microfiles are secured when Remote Access is used is described in the Richtlijnen voor Remote Access-output. In addition, CBS has regels for the use of the Remote Access facility and a maatregelenbeleid, and it lays down conditions for the use of the Remote Access facility in a project agreement.

Prior to any processing, a risk analysis of the privacy and security aspects is carried out. This is done on the basis of a Baseline assessment of privacy protection and information security. The aim

of this assessment is to determine whether sufficient measures have been taken for a specific process to reduce the risks in the area of privacy and information security to an acceptable level. In other words, it is assessed whether the process meets the requirements of privacy and security standards.
The first part of the assessment is a checklist containing a number of standards in the area of privacy protection and information security (baseline). Here, it is assessed whether the set standards are being met and whether the associated control measures have been correctly and fully implemented. The second part of the assessment is the question whether, in addition to the generic measures, specific measures have been taken for this process (baseline assessment). Specific measures may be required, for example, due to the nature or design of the process or the number of people involved. If specific measures have been taken for the process, it should be argued, based on a risk assessment, that these adequately cover the risks identified. The Baseline Assessment is evaluated annually.

In addition to external audits, CBS also has a system of internal audits. A report on the internal audits is submitted annually to the Executive Board of CBS.

You can add additional points here: select the tab *Invoegen*, choose *Snelonderdelen, Aanvullend punt*

Add a concluding paragraph here, if desired. For example:
- Lessons from this PIA
- Next steps, etc.


Maatregelen
nemen
Privacybewustwording
Doelbinding
PIA
Noodzaak
Effecten in kaart
Bescherming van
persoonsgegevens
Risico's
minimaliseren
Richtinggevend
Rechtsgrond
Met open vizier