DANMARKS STATISTIK

Statistics Denmark’s Information Security Policy

We take good care of data in the digital world

Statistics Denmark is the central producer of statistics in Denmark and has many years of experience in processing data for the purpose of documenting conditions in society. Statistics Denmark operates on the basis of our core values of independence, trustworthiness, user orientation and data security.

In accordance with these values, and to uphold the digital confidence the public has placed in us, we are continuously focusing on information security. Developments in information technology result in drastically increasing volumes of data. In Statistics Denmark, we are continuously working in response to this to develop our procedures and security mechanisms to protect data. The population and the users of our services must always be able to trust that data is in safe hands.

Statistics Denmark, March 2021

Birgitte Anker
Director General

Contents

1 Introduction

This is Statistics Denmark's information security policy, which establishes the framework of the security work in Statistics Denmark in compliance with the national information security standard ISO 27001.

Moreover, we refer to the general information security policy of the Danish Ministry of the Interior and Housing, which applies to all of the ministry's areas of responsibility.

For the purpose of this policy, *information security* is defined in a wider sense than data security and is a commonly used term in the Danish government's security management. Information security means the required protection of all resources included in or contributing to Statistics Denmark's processing and communication of information, whether in electronic form, paper form etc. – including technology and organisational processes.

Statistics Denmark's information security policy is based on requirements identified in:

- The Statistics Denmark strategy in force at any time, currently Strategy 2022
- Provisions, legislation/regulations and directives etc. within Statistics Denmark's domain, including ISO 27001 and the General Data Protection Regulation (GDPR)
- The present and expected threat landscape relating to information security.

On the basis of systematic risk assessments and a concrete probability analysis and impact assessment, Statistics Denmark must ensure the level of security decided by Statistics Denmark's Executive Board and in correspondence with the value of the information assets in Statistics Denmark.
Moreover, Statistics Denmark has implemented an ISO 27001-based Information Security Management System, ISMS, and has considered the controls in Annex A of the ISO 27001 standard in the form of a Statement of Applicability (SoA), which has been extended with a set of specific Statistics Denmark controls.

The information security policy is to create the framework for a series of specific rules, guidelines and procedures that contain an efficient control environment. In this way, a foundation is established for the day-to-day work with information security in Statistics Denmark.

The information security policy is an important part of Statistics Denmark's information security handbook and describes the management-approved level of security.

Statistics Denmark's information security policy describes the importance of the work with information security in Statistics Denmark and determines the level of ambition for this work. Accordingly, the information security policy contains the overall security objectives and creates a basis for the drawing up of Statistics Denmark's information security handbook, which is to be understood as the generic term for the information security policy with the underlying series of guidelines and procedures.

Key Statistics Denmark documents and policies concerning information security of interest to external stakeholders (incl. this information security policy) are also published on Statistics Denmark's website and can be found at https://www.dst.dk/da/OmDS/datasikkerhed-i-danmarks-statistik/.

2 Statistics Denmark's information security objectives

It is Statistics Denmark's objective to maintain a high level of information security, which is at the very least level with that of comparable institutions. The objective of a high level of security is balanced with the desire for an expedient and user-friendly application of IT and general financial resources.

The requirements to information security are assessed in relation to their relevance to Statistics Denmark, thus maintaining focus on a level of information security where common sense and regard for the public's legitimate need for and expectation of secure management of data and assets are key factors. In addition, data and systems are secured based on an assessment of what is necessary, with due consideration of the financial framework.

The purpose of our information security is to:

- Facilitate confidential processing, transmission and storage of data, e.g. by using de-identification/pseudonymisation and encryption of data to the widest extent possible.
- Provide operational security and minimum risk of critical failures
- Support compliance with the General Data Protection Regulation (GDPR), also as a data processor for others
- Prevent loss and leakage of data
- Prevent identification of individuals and sole proprietorships, e.g. through de-identification and statistical disclosure limitation
- Prevent fraud by means of automated and manual control measures
- And building on this, obtain correct functioning of the IT systems with a minimum risk of tampering with data and systems. I.e. means for this purpose must be available and applied according to specific needs
- Safeguard against attempts to bypass security measures
- Support awareness of information security internally and externally, so that all employees and external users are aware of and relate to information security in their day-to-day work

Moreover, it should be pointed out that Statistics Denmark does not control systems with personal data as defined by the Ministry of Justice to be subject to storage exclusively in Denmark (the location requirement in the Data Protection Act).

Statistics Denmark does not only see a high level of security as a requirement to comply with legislation and regulatory requirements, but also as an element of quality to be able to provide a reliable service for citizens and data reporting offices. In other words, information security is an explicit key value with Statistics Denmark of a strategic nature and is included as a separate topic in Strategy 2022. Information security must be an integral part of IT activities in Statistics Denmark.

Statistics Denmark was ISO 27001 certified in 2020 with the scope of statistics production and associated IT and business processes, serving as documentation of a high level of security

In addition, Statistics Denmark has ISAE 3000 reports issued on a regular basis to document its compliance with GDPR (the General Data Protection Regulation).

3 Scope of the policy

The scope of the information security policy is defined as follows:

- The information security policy applies to everybody working for Statistics Denmark irrespective of employment status, including external consultants and service employees.
- The information security policy applies to all systems and any data in Statistics Denmark's possession.
- Suppliers and cooperating partners with physical or logical access to Statistics Denmark's systems and data must also be familiar with and comply with the information security policy.
- The information security policy covers all technical and administrative matters that directly or indirectly influence the operation and use of Statistics Denmark's IT systems, data and paper archives.
- The information security policy is approved by the Executive Board and is reassessed annually to ensure that it complies with the security objectives pursued by Statistics Denmark.

4 Non-compliance with the policy

All employees are personally responsible for compliance with Statistics Denmark's information security procedures and agree to this by their signature when they are appointed.

Everyone working for Statistics Denmark is obliged to comply with the current information security policy including guidelines, business practices and related appendices. Non-compliance may involve sanctions.

The sanctions may be related to employment law, law of torts and/or criminal law, depending on the circumstances and the situation.

If an employee is aware of any non-compliance with Statistics Denmark's information security policy, the employee must report it without delay to the information security coordinator, the director of User Services or the Service Desk.

5 Organisation and responsibilities

The Executive Board is responsible for working with information security at a strategic level, so that information security is an integral part of all significant decisions. Managers and employees are responsible for complying with guidelines and procedures for security in their day-to-day work.

Statistics Denmark's management (Executive Board) defines the planning, implementation and control of information security. The information security coordinator is responsible for the implementation and maintenance of the information security system in Statistics Denmark and for the follow-up on security incidents.

The Executive Board must reassess, update and approve the information security policy annually, or in connection with any situations that call for it, such as major changes in responsibilities.

Statistics Denmark has set up an information security committee with reference to the Executive Board. The chair of the committee is a director (of User Services) and the remaining members represent all departments as well as IT.

Statistics Denmark has an information security coordinator who is part of the IT staff, but refers to the chair of the information security committee in matters of information security. The current day-to-day work is handled by IT and the IT security group, which is supported by Statistics Denmark's governance model in the area of security.

Statistics Denmark has designated system owners who are professionally accountable for Statistics Denmark's systems. The system owners are typically the heads of IT as well as heads of statistical divisions. They must ensure that their systems comply with the current information security procedures. Furthermore, the system owners must ensure compliance with GDPR (the General Data Protection Regulation) and supervise data processors.

6 Security awareness

All Statistics Denmark employees are responsible for the information security. They must be familiar with and comply with Statistics Denmark's information security policy, information security handbook, rules and procedures of Statistics Denmark.

The required knowledge and competence regarding information security must be communicated to all employees, and their attitudes, culture and knowledge regarding information security must be developed on a continuing basis. This should take place in connection with the onboarding, at introductory courses and in the form of regular awareness campaigns as described in the concept devised for information security awareness.

7 Data confidentiality policy

Confidentiality in the handling of statistical products and other data material is about protecting the statistical units against disclosure of information requiring confidentiality. This applies with respect to the surrounding world as well as Statistics Denmark's employees.

The rules of enforcement of data confidentiality are implemented in a data confidentiality policy with necessary guidelines for dissemination and statistical disclosure limitation as well as for determination of individual access rights to confidential information in Statistics Denmark. The data confidentiality policy is governed by the Data Confidentiality Committee.

8 Information security handbook

A series of guidelines and procedures provide details on the information security policy. In combination, the policy, guidelines, contingency policy and procedures constitute the information security handbook.

The guidelines that are relevant for the employees of Statistics Denmark are available on the intranet.

The day-to-day operational responsibility for maintaining the information security handbook lies with the information security coordinator and the IT security group in IT. Material for the information security handbook must obtain approval from the Information Security Committee, which refers to the Executive Board.

The information security coordinator is responsible for managing the documentation that is part of Statistics Denmark's information security handbook or that in some other manner supports the management system for information security in Statistics Denmark, in particular ensuring regular review and updating of the documents.

9 Level of security

Independence, trustworthiness, user-orientation and data security are core values for Statistics Denmark. Data security is an important strategic area of priority.
A sufficient level of information security is obtained through security measures ensuring:

1. Confidentiality, integrity/authenticity (non-repudiation) and availability of Statistics Denmark's systems and data in relation to the IT risk assessment determined for the individual system/set of data:

   Confidentiality: Statistics Denmark must continuously ensure that it processes collected data in a secure manner. Statistics Denmark must make provisions for secure processing, transmission and storage of data and prevent any loss of data. The security measures must protect data against misuse and unauthorised access to information about individuals and enterprises. In that respect, Statistics Denmark has the strategic goal of applying de-identified data to the maximum extent possible.
   Integrity: Statistics Denmark is continuously working on ensuring reliable and correct functioning of the systems with a minimum risk of incorrect base data and consequently statistics, e.g. due to human errors or system errors. For this reason, the work to ensure the high quality of Statistics Denmark's documentation and testing of the systems is an ongoing process.
   Availability: Statistics Denmark is continuously working to achieve high availability through high uptime and minimised risk of outages. In accordance with Strategy 2022, Statistics Denmark is working digitally to a still higher degree. This applies to services, processes, data and statistical cooperation. For this reason, the availability of the systems is of increasing strategic importance. The Executive Board decides the level of the systems' availability.

2. Protection of Statistics Denmark's IT assets, employee competences, public image and information/data in Statistics Denmark's possession.

To maintain an adequate level of security in Statistics Denmark, the following must be observed:

- Detailed guidelines and procedures must be available and ensure that information security is an integral part of Statistics Denmark's operation and day-to-day routine.
- In its contract and supply management, Statistics Denmark must ensure that the use of external consultants, collaboration partners and suppliers complies with Statistics Denmark's information security level.
- Follow-up on information security is necessary – for more information, see section 13 "Follow-up".

10 Risk assessment and classification

It is Statistics Denmark's policy to have a risk-based approach to information security according to ISO 27001. This means that Statistics Denmark actively responds to existing risks and decides on measures to counter risks.

Risk assessment at the operational level
The information security in Statistics Denmark must take due account of regulatory requirements, contractual obligations as well as obligations towards parties that are required to use Statistics Denmark. It is Statistics Denmark's stated objective to be aware of relevant risks and to respond to these in the light of Statistics Denmark's financial capabilities.

A concept has been specified for performance of risk assessments and recording of observations.

Every year, a number of risk assessments are made of the most critical systems, i.e. the business-critical systems and systems that are crucial to society, as agreed with the management (the Information Security Committee), and in connection with any major changes in tasks, suppliers, IT systems or use thereof. Before any commissioning of new technology, such as Cloud-based systems, Statistics Denmark must carry out a risk assessment of the use of such technology.

The Executive Board reviews the risk assessment and is responsible for preparing a security strategy that prevents unacceptable risks relative to financial capabilities.

Classification:
Statistics Denmark has access to large volumes of data about citizens and companies, and much of this information is of a confidential nature. In accordance with the Danish Criminal Code and the Danish Public Administration Act, a certain part of the statistical information in Statistics Denmark will be confidential. However, Statistics Denmark has chosen to classify all statistical information as confidential in order to ensure a consistently high level of confidentiality.
Likewise, not yet published material and e.g. material of a staff-related nature is also regarded as *confidential information*.

Confidentiality is ensured e.g. through the application of internationally recognised methods in the form of anonymisation/pseudonymisation and encryption.

For further information and rules, see the data confidentiality policy.

11 Emergency planning

According to section 24, subsection 1, of the Danish Emergency Management Act, the ministers are obliged to ensure that adequate emergency planning is effected within their respective areas of responsibility. Testing of the emergency plan and completion of exercises are a part of this obligation. Conducting exercises helps reinforce the crisis management preparedness and build up a crisis management routine in Statistics Denmark, and it may help uncover any weaknesses in the emergency plan. Exercises are also important for testing that the organisation, plans and procedures are effective.

For this purpose, Statistics Denmark must have an IT emergency plan that will be deployed in case of information security disasters and incidents, such as long-term crashes, power failures, fire, etc. The IT emergency plan must ensure that the systems can be restored so that they can continue to operate.

As an element in restoring Statistics Denmark's systems and ensuring continued operation, Statistics Denmark must provide for external emergency services, which means that the most important systems can continue to run on an external fallback site.
Systems within the framework of the emergency services have been selected and defined by the Information Security Committee.

Furthermore, Statistics Denmark must ensure continued operation in a period of power failure by having an emergency power plant that can keep Statistics Denmark's IT environment going for a period.

12 Non-compliance and internal supervision

Non-compliance
If situations arise in which Statistics Denmark is unable to comply with the requirements of the information security policy, a written request for exemption must be submitted to the chair of the Information Security Committee. Any non-compliance with the requirements must be documented and alternative security measures must be implemented.
However, emergencies are taken into consideration where acute crises may involve temporary non-compliance that must be handled on the spot. Such instances must subsequently be reported to the chair of the Information Security Committee.

Internal supervision
According to ISO 27001 and Statistics Denmark's information security strategy, the responsibility for the information security and accordingly the internal supervision lies with the management, especially the Director of User Services.

Internal supervision is performed to identify whether there is a common thread running through Statistics Denmark's ISMS, from risk picture, senior management decisions and the overall information security policy to the underlying information security policies and procedures that must fulfil the information security requirements and to the implemented controls.

The internal supervision must always be independent, as described in the concept for the internal supervision.

The internal supervision consist in drawing a selection of samples and collecting testimonials from interviews, review of project documents, the management system's documents and related processes. Any deviations uncovered in connection with performance of the internal supervision are recorded and processed in the context of the general risk management.

The internal supervision reports to the Information Security Committee, whose members also decide who become part of the supervision team.

13 Follow-up

Statistics Denmark measures and follows up on the information security in the following way:

1. Statistics Denmark must follow up on the information security by continuously optimising the management system through regular maintenance and optimisation of the information security strategy, the information security policy and the associated rules and procedures. The aim is to maintain a structured and continuing improvement process and ISO 27001 certification in selected areas.
2. The department of the relevant ministry and the Office of the Auditor General of Denmark, Rigsrevisionen, conduct independent third-party audits and supervision.
3. Risk assessments are made on a regular basis where impartial external consultants are involved as necessary.
4. An annual security test is made of Statistics Denmark's external use systems to identify any risks of system intrusion etc.
5. Continuous recording and follow-up on incidents within the sphere of information security.
6. The director of User Services and subsequently the Information Security Committee are informed of all incidents. In the event of critical failures, IT prepares a report for the Executive Board regarding consequences, reasons and solutions.

14 Maintenance and effective date

Changes in the security documentation are handled in the following way:

- The information security policy must be approved by the Information Security Committee and the Executive Board. The policy must be maintained at regular intervals, meaning once a year at the very least.
- The information security handbook, including relevant appendices and guidelines, must be approved by the Information Security Committee. Key procedures must be reviewed and maintained at regular intervals.
- Operational procedures must be maintained and approved by the IT security group.

This information security policy has been approved at the Information Security Committee meeting on 10 December 2020 and by the Executive Board on April 8th 2021, after which it has become effective.