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 processed confidential data for many years for the purpose of documenting conditions in society. Statistics Denmark operates on the basis of our core values of trustworthiness, openness, user-orientation, adaptive capability and data accountability.

To uphold the digital confidence the public has placed in us, we are continuously focusing hard on information security. In a world characterised by high risks and constant change, information security remains one of our top priorities.

Developments in information technology result in drastically increasing volumes of data and many challenges with respect to data security. In Statistics Denmark, we are continuously working in response to this to develop the procedures and security mechanisms we have set up to protect our vast volume of data. The population and the users of our services must always be able to trust that data is in safe hands.

Statistics Denmark April 9th 2025

Martin Ulrik Jensen
Director General

Contents

1 Introduction

This is Statistics Denmark's information security policy, which establishes the framework of the security work in Statistics Denmark and complies with the information security standard ISO 27001:2022.

Moreover, we refer to the general information security policy of the Danish Ministry of Digital Affairs, which applies to all of the ministerial areas of responsibility.

The term information security must be understood in a wider sense than data security and is a term used in the central government security management. Information security means the required protection of all resources included in or contributing to Statistics Denmark's processing and communication of information. This applies whether in electronic form or paper form, and technology and organisational processes are also included.

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

- The strategy of Statistics Denmark in force at any time, currently Strategy 2025
- Provisions, legislation/regulations and directives etc. within Statistics Denmark's domain, including ISO 27001 and the General Data Protection Regulation (GDPR)
- The present and anticipated security alert status and resulting requirements from external partners and stakeholders, such as the Centre for Cyber Security.

On the basis of systematic risk assessments and a concrete probability and impact assessment analysis, Statistics Denmark must ensure the level of security decided by Statistics Denmark's Executive Board and corresponding 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 standard in the form of a Statement of Applicability (SoA), which has been extended with a set of specific Statistics Denmark measures.

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 the organisation and determines the level of ambition in this respect. Accordingly, the information security policy contains the overall security objectives and provides the basis for drawing up Statistics Denmark's information security handbook, which is to be understood as the generic term for the information security policy with the underlying rules 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 are currently available at https://www.dst.dk/en/OmDS/datasikkerhed-i-danmarks-statistik/.

2 Information security objectives in Statistics Denmark

Statistics Denmark aims to maintain a high level of information security that is at a minimum 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 against their relevance to Statistics Denmark, thus maintaining focus on a level of information security where good 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 must be secured based on an assessment of what is necessary, with due consideration of the financial framework.

Information security rests on three major cornerstones concerning data confidentiality, data integrity and data availability (in the data systems). Confidentiality means that information is shown only to those who have the rights to see the relevant data. Integrity comprehends that data is correct and availability means that data is accessible, i.e. that systems are up and running.

Statistics Denmark's information security objectives are anchored in confidentiality, integrity and trustworthiness, and accordingly state that:

1. **confidential information, including all non-published statistical data, is protected** against unauthorised access.

This includes e.g.:

- confidential processing, transmission and storage of data, e.g. by means of de-identification/pseudonymisation and encryption,
- prevention of identification of individuals and sole proprietorships, e.g. through de-identification and statistical disclosure control as described in Statistics Denmark's Data Confidentiality Policy
- prevention of loss and leakage of data
- support of compliance with the General Data Protection Regulation (GDPR), including as a data processor for others

2. **all information**, statistical data as well as non-statistical data, **is correct and complete** and that IT systems are working properly.

This includes e.g.:

- automated and manual control measures to prevent e.g. fraud
- ensuring the proper functioning of the IT systems with a minimum risk of tampering with data and systems

3. **all information**, both statistical data and non-statistical data, and IT services are **available**.

This includes e.g.:

- ensuring operational security and minimising the risk of critical IT failures, e.g. as a result of cyberterrorism and attacks on infrastructure.

In support of all three objectives, Statistics Denmark focuses resources on raising awareness of information security internally as well as externally, so that all employees and external users are aware of and address information security in their daily work.

Aside from that, 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, data accountability is an explicit key value of a strategic nature to Statistics Denmark and is included as a separate topic in Strategy 2025.

Statistics Denmark was ISO 27001 certified for the first time in 2020 with the scope of statistics production and associated IT and business processes, serving as documentation of a high level of security, and external auditors follow up on this annually. In 2023, Statistics Denmark was recertified and switched to ISO 27001:2022. External auditors follow up annually on Statistics Denmark's certification.

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 information security policy applies to everybody working for Statistics Denmark irrespective of employment status, including external consultants and service employees, just as it applies to all systems and all 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.

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 procedures 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 to the information security coordinator, the director of User Services or Service Desk without delay.

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.

The 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 information security

coordinator is part of the IT staff, but in matters of information security, he or she refers to the chair of the information security committee. The current day-to-day work is handled by IT and the IT Security Group.

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 areas of responsibility.

Statistics Denmark has set up an Information Security Committee that reports 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.

6 Security awareness

All of 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.

The required knowledge and competence regarding information security must be communicated to all employees, and we must persistently work on attitudes, culture and knowledge regarding information security. This must be done 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 for enforcement of data confidentiality are implemented in a data confidentiality policy with necessary guidelines for dissemination and statistical disclosure control as well as allocation 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 set of guidelines and procedures provide details of the information security policy. In combination, the policy, guidelines, contingency policy and business 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.

It is the responsibility of the information security coordinator to manage documentation that is part of Statistics Denmark's information security handbook or otherwise supports the management system for information security in Statistics

Denmark, in particular to ensure that the documents are reviewed and updated regularly.

9 Level of security

Statistics Denmark is working with a high level of security to ensure that public data is sufficiently protected. The executive board decides the level of security, and they address the subject once a year at the minimum.

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

- Detailed guidelines and business 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 is in compliance with Statistics Denmark's information security level.
- Follow-up on information security is necessary

10 Risk assessment

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.

The Executive Board reviews the overall risk assessment and is responsible for preparing a security strategy that prevents unacceptable risks with due consideration of financial capabilities.

The executive board makes decisions about the handling of risks affecting the strategic goals of Statistics Denmark, its resources, organisation or reputation.

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 the 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 established for performance of risk assessments and recording of observations. Among other things, the risk assessments address GDPR legislation, legacy, security breach, vulnerabilities, need for logging, deployment of new technology, and other issues of relevance to the individual area of activity.

Every year, a number of risk assessments are made as agreed with the director of User Services, e.g. via the collaborative fora in which the director takes part. The assessments will typically be made in connection with major changes in tasks, suppliers, IT systems or the use thereof or in response to external risks.

Deployment of new technology
The public interest is high on the agenda when Statistics Denmark deploys new technology to be applied for confidential data and information, both in the statistical production and for administrative data.

Risk assessments must be prepared, in particular when and if applying, for example, cloud-based systems, AI solutions or solutions involving use of internet-based services or sharing of information and data. Statistics Denmark's management wants such solutions to be considered explicitly and, for this reason, risk assessments, impact analyses and similar assessments as well as executive board presentations must be completed before implementation.

New technology can be taken to mean technology and tools where statistical data and other confidential information is processed[1] in an application or system or by a method or process that is newly developed and not previously applied in Statistics Denmark. Or where the technology has the potential to transform ways of working, change behaviour patterns or affect society in various ways.

In connection with risk assessments of new technology, it is considered how the new technology will affect Statistics Denmark's established information security setup, just as consequences must be considered for the users and businesses whose data Statistics Denmark is using. This means that consideration is given to which new risks a technology may introduce and where new security measures should be implemented to match and safeguard the existing high level of security.

11 Data 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 is 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.

12 Emergency planning

Statistics Denmark's IT emergency plan will be deployed in case of information security incidents and disasters, such as long-term crashes, power failures, fire, etc. The IT emergency plan must ensure that the systems can be restored, so that operations can continue.

As an element in restoring Statistics Denmark's systems and ensuring continued operations, Statistics Denmark must provide for external emergency services, which means that the most important systems can continue to run on an external fallback site.

[1] Processing, such as collection, recording, organisation, systematisation, storage, alignment or change, retrieval, search, use, passing on via transmission, dissemination or any other kind of handing over, compilation or linkage, delimitation, deletion or destruction.

Systems to be comprised by the emergency services are recommended by the Information Security Committee and subsequently presented to the Executive Board.

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

13 Non-compliance and internal supervision

Non-compliance
If situations arise where the requirements in the information security policy cannot be observed, 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 account 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
The responsibility for the information security and accordingly for the internal supervision lies with the Executive Board, especially the director of User Services.

Internal supervision is carried through to identify whether there is a common thread running through Statistics Denmark's ISMS (Information Security Management System), from risk picture, senior management decisions and the overall Information Security Policy to the underlying information security policies and procedures that must meet 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, reviewing project documents, the management system documents and related processes. Deviations detected in the process of the internal supervision are recorded and treated in connection with the general risk management.

The internal supervision reports to the Information Security Committee, who also approves the staffing of the supervision team.

14 Follow-up

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.

The department in the relevant area of responsibility and the Office of the Auditor General of Denmark, Rigsrevisionen, conduct independent third-party audits and supervision, and risk assessments are made on a continuing basis, involving impartial external consultants as needed.

An annual security test is made of Statistics Denmark's external use systems to identify any risks of system intrusion etc.

The information security coordinator conducts continuous recording and follow-up on incidents in the field of information security. The chair of the information security committee, and subsequently the rest of the information security committee, is briefed on all incidents. In the event of critical failures, IT prepares a report for the Executive Board regarding consequences, reasons and solutions.

15 Maintenance and effective date

The information security policy is approved by the information security committee and the Executive Board and is reassessed at a minimum once a year to ensure that it complies with the security objectives pursued by Statistics Denmark.

The information security handbook, including relevant appendices and guidelines, has been approved by the Information Security Committee. Major changes need pre-operational approval by the committee. Operational procedures and minor changes to the information security handbook are maintained and approved by the IT Security Group.

The information security policy was reviewed at the Information Security Committee meeting on 14 January 2025 as well as by the Executive Board on April 9th 2025, after which it became effective.