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 to document conditions in society. Statistics Denmark operates based on a set of core values, which are independence, trustworthiness, user-orientation and data security.

In accordance with these values, and to uphold the digital confidence the public shows us, we are continuously focusing on information security. Developments in information technology result in 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 2020

Jørgen Elmeskov
Director General

Contents

1 Introduction

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

Moreover, we refer to the general information security policy of the Danish Ministry for Economic Affairs and the Interior, which applies to all of the ministry's area 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 DST's processing and communication of information, whether in electronic form, paper form etc. – including technology and organisational processes.

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

- The DST Strategy applicable at any time, currently Strategy 2022
- Provisions, legislation/regulations and directives etc. within DST'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, DST must ensure the level of security decided by DST's Executive Board in correspondence to the value of the information assets in DST.
Moreover, DST 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 DST 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 DST.

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

DST's information security policy describes the importance of the work with information security in DST 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 DST'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 DST documents and policies concerning information security of interest to external stakeholders (incl. this information security policy) are also published on DST's website and can be found on
http://www.dst.dk/en/OmDS/lovgivning/.

2 DST information security objectives

It is DST'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 DST, 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:

- Obtain the possibility of confidential processing, transmission and storage of data, e.g. by using anonymisation/pseudonymisation and encryption of data to the widest extent possible.
- Obtain a high level of operational availability and minimum risk of major outages
- 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 confidentialisation
- Prevent fraud by means of automated and manual control measures
- 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

DST 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 DST and is included as a separate topic in Strategy 2022. Information security must be an integral part of DST's IT activities.

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 DST irrespective of employment status, including external consultants and service employees.
- The information security policy applies to all systems and any data in DST's possession.
- Suppliers and cooperating partners with physical or logical access to DST'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 DST'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 DST.

4 Non-compliance with the policy

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

If an employee is aware of any non-compliance with DST's information security policy, the employee must report it to the information security coordinator, the director of User Services or the Service Desk without delay. Depending on the situation, it may have consequences for the staff.

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.

DST'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 DST 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.

DST has appointed 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 divisions as well as IT.

DST 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 the DST governance model in the area of security.

DST has designated system owners who are professionally accountable for DST's systems. The system owners are typically the heads of IT as well as heads of statistical sections. They must ensure that their systems comply with the current information security procedures.

All employees are personally responsible for compliance with the DST information security procedures and agree to this by their signature when they are appointed.

6 Security awareness

Everyone working for DST is responsible for the information security. They must be familiar with and comply with DST's information security policy, information security handbook, rules and procedures of DST.

The required knowledge and competence regarding information security must be communicated to all employees, and attitudes, culture and knowledge regarding information security must be developed on a continuing basis, taking place in connection with onboarding, at introductory courses and in the form of regular awareness campaigns.

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 disclosure and confidentialisation 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. In addition, a series of guidelines relevant for IT employees is available on a network drive to which IT employees have access.

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 the DST information security handbook or that in some other manner supports the management system for information security in DST, including ensuring regular review and updating of the documents.

9 Level of security

Independence, trustworthiness, user-orientation and data security are core values for DST. 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 DST's systems and data in relation to the IT risk assessment determined for the individual system/set of data:

   Confidentiality: DST must continuously ensure that it processes collected data in a secure manner. DST 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, DST has the strategic goal of applying de-identified data to the maximum extent possible.
Integrity: DST 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 DST's documentation and testing of the systems is an ongoing process.
Availability: DST is continuously working to achieve high availability through high uptime and minimised risk of outages. In accordance with Strategy 2022, DST 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 DST's IT assets, employee competences, public image and information/data in DST's possession.

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

- Detailed guidelines and procedures must be available and ensure that information security is an integral part of DST's operation and day-to-day routine.
- In its contract and supply management, DST must ensure that the use of external consultants, collaboration partners and suppliers complies with DST'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 DST's policy to have a risk-based approach to information security according to ISO 27001. This means that DST actively responds to existing risks and decides on measures to counter risks.

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

Every year, we make a number of risk assessments 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 major changes in tasks, suppliers, IT systems or use thereof. Before any commissioning of new technology, such as Cloud-based systems, DST 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:
Any data and information in which individuals and/or enterprises are identifiable, is regarded as confidential information. Not yet published material and material of a financial, staff-related or strategic nature in the course of prepara-

tion as well as other administrative information is also regarded as *confidential information*.
Confidentiality is ensured e.g. through the application of internationally recognised methods (such as 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 DST, 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, DST must have an IT emergency plan that becomes effective 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 DST's systems and ensuring continued operation, DST must provide for external emergency services, which means that the most important systems can continue to run on an external fallback site. This covers e.g. operation of the website, data banks and the Law Model as well as data sharing solutions, even if DST's IT environment at the physical site should be unavailable.

Moreover, DST must ensure continued operation during a power failure by having a backup power supply system that can keep DST's IT environment running for a period.

12 Non-compliance and internal supervision

Non-compliance
If situations arise in which DST 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, including the Director of User Services. A superior officer has been designated as responsible and reports to the director of User Services in matters of security, and he or she must establish and maintain a complete overview of DST's internal supervision.

The internal supervision must ensure that an overall internal supervision plan is prepared and maintained based on the SoA document. Furthermore, the supervision must ensure that the internal supervision is conducted at the stated intervals for each SoA control, that it is documented and that the results of the supervision are followed-up. The supervision is based on random checks within the designated areas and on review and assessment of the reports created based on the logging.

Finally, it must be ensured that the results of the internal supervision is reported to management and to the Information Security Committee in connection with the ordinary and any extraordinary meetings.

The information security coordinator has been designated as the person responsible for planning the internal supervision.

Non-compliance ascertained in connection with the execution of the internal supervision is registered and processed in conjunction with the general risk assessment.

13 Follow-up

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

1. DST 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 objective is to ensure 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. An annual risk assessment is made where impartial external consultants are involved as necessary.
4. An annual security test is made of DST's systems for external use to identify any risks of system intrusion etc.
5. Continuous registration 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 11 December 2019 and by the Executive Board on 11 March 2020, after which it has become effective.