



Information Security and Data Protection Policy

Adopted by the Grant Thornton Sweden AB Board of Directors 25 August 2026

Valid from 1 September 2026

Policy owner: Chief Information Officer

Information classification: Open

1. Introduction and purpose

The *Information Security and Data Protection Policy* of Grant Thornton Sweden AB and its subsidiaries (“Grant Thornton”), together with the *Code of Conduct*, our success factors and other governing documents, shall contribute to the success of the companies and the achievement of their goals. The purpose of the policy is to increase quality, ensure compliance with legal requirements and underpin the companies’ strategy and vision by establishing information security and data protection principles. The policy is an important part of the companies’ quality, risk, compliance and sustainability management.

Grant Thornton handles large amounts of information, both within the context of client activities and internally. External and internal rules on auditing, professional ethics and data protection define high standards regarding the security of both business information and personal data.

2. Scope

Pursuant to decisions made by the respective Board of Directors, this policy applies to all persons who work for or on behalf of Grant Thornton Sweden AB and its subsidiaries, including employees, trainees and, where applicable, external consultants. All of these are referred to as employees in governing documents.

The policy shall be applied in the same way across all subsidiaries after implementation, while ensuring applicable local legislation and relevant regulatory frameworks are also taken into account. In cases in which binding local legislation or regulations necessitate exceptions to this policy, such exceptions require the approval of the policy owner.

The “Supplier Code of Conduct” applies to suppliers and other partners.

Roles and responsibilities are described at an overall level in Grant Thornton’s Governance framework.

Focus areas in this policy

- Roles and responsibilities relating to information security
- Roles and responsibilities relating to data protection
- Appropriate protection of information and personal data
- Internal logging of various types of incidents relating to information security and data protection

3. General regulatory compliance

Grant Thornton shall comply with all the applicable laws of the countries and jurisdictions in which the companies operate, as well as, to the extent applicable, the standards and international guidelines relating to the areas covered by this policy, including standards issued by Grant Thornton International Limited (“GTIL”).

4. Training, guidance and awareness-raising activities

Grant Thornton shall strive to raise awareness about the content of the policy among its employees. Training, guidance and communication activities shall be relevant and tailored to the specific roles and organisational affiliations. The implementation of training activities shall be monitored and assessed quantitatively and qualitatively.

5. Information security and data protection activities at Grant Thornton

Grant Thornton’s risk-based work with information security and data protection is based on applicable data protection legislation as well as international information security standards and guidelines, Grant Thornton’s global information security framework and internal policies relating to information security and data protection. The purpose is to enable us as a company to comply with relevant regulations and provide appropriate protection of the information and personal data handled in the business, and to achieve a good culture regarding information security and data protection.

Fundamental elements of information security and data protection are that there shall be clear roles and management responsibilities that underpin the ensuring of appropriate protection of information and personal data, and that various types of incidents relating to information security and data protection shall be logged and handled internally.

Grant Thornton shall work actively with information security activities in order to protect Grant Thornton’s information assets in an appropriate manner, reduce the risk of misuse of business information and prevent IT-related disruptions that may adversely affect business activities. The protection that is implemented shall be adapted to the nature, scope and risk involved, taking into account both external and internal requirements defined in laws, regulations and internal governing documents.

Grant Thornton shall work actively with data protection activities in order to ensure good compliance with applicable data protection legislation, and maintain appropriate organisational and technical protection for personal data that is processed. A good data protection culture is an important part of the overall information security culture.

5.1. Roles and responsibilities relating to information security

All employees have a responsibility to ensure good information security in their daily work. Within Grant Thornton, the CEO is ultimately responsible for information security and compliance with information security requirements at Grant Thornton. The operational responsibility for information security and information ownership resides with the relevant managers at the respective business areas and Corporate Functions. In addition, Grant Thornton shall appoint a Chief Information Security Officer (CISO).

5.1.1. A good information security culture

A good information security culture means that all employees shall be aware of their own particular responsibility for information security and which rules are applicable, and have the ability to recognise events that could have an adverse impact on information security. By providing training and information, all employees shall be made aware of information security issues, as this underpins compliance and promotes a good information security culture.

5.2. Roles and responsibilities relating to data protection

All employees have a responsibility to maintain an appropriate level of protection for the personal data that is processed in the context of their daily work. Within Grant Thornton, the Board of Directors is ultimately responsible for ensuring that personal data is processed in accordance with the applicable data protection legislation. The operational responsibility for ensuring compliance with data protection rules is linked to the information ownership (see section 5.1). Grant Thornton shall appoint a Data Protection Officer (DPO). The authority and fundamental tasks of this role are defined in the applicable data protection legislation.

5.2.1. A good data protection culture

Grant Thornton shall work actively with data protection to ensure compliance with data protection regulations when personal data is processed as part of Grant Thornton's business operations. It is important that the fundamental principles regarding the processing of personal data are respected. Data protection measures shall form an integral part of the daily business activities. By providing training and information, all employees shall be made aware of data protection issues, as this underpins a high level of protection for the personal data that is processed and promotes a good data protection culture.

5.3. Appropriate protection of information and personal data

All information handled in the business shall be classified and personal data processing operations shall undergo risk analysis to ensure an appropriate level of protection for both information and personal data. Appropriate protection shall be ensured throughout the entire lifecycle, i.e. during the definition of requirements prior to procurement, as well as during implementation, use/processing, development and finally the decommissioning of information systems/IT support. Appropriate safeguards shall, when required, also include risk-based background checks. The companies shall have insight into and control over the supply chain to ensure that all parties are compliant with the security and data protection requirements.

5.3.1. Responsible use of digital tools and services

Digital tools and services are used in both client-facing and internal business activities to support the handling of large volumes of information and personal data. These tools and services, including various AI solutions, must be evaluated both before the tools and services are put into use and on an ongoing basis while they are being used. This is intended to ensure appropriate protection of information and personal data. There is also an obligation to maintain statutory confidentiality when a client's information is processed using digital tools and services. Applicable laws and regulations shall be observed, to ensure responsible use of tools and services.

Commonly available and free digital tools and services often entail an increased risk due to shortcomings regarding protection of the information and personal data that is shared or used in such tools or services.

5.4. Internal logging of various types of incidents relating to information security and data protection

Incident management forms part of the regular and systematic information security and data protection activities. Grant Thornton shall manage all incidents that occur, address any shortcomings and regularly follow up incidents to ensure a high level of protection for both business information and personal data. An important aspect of this work is being informed of any incidents that occur in daily operations, and this requires that all employees have the knowledge and skills needed to detect incidents. There shall be a process for internal logging of incidents that could involve security incidents or personal data incidents.

6. Compliance and monitoring

The policy owner is responsible for ensuring satisfactory implementation of the policy, which includes:

- Developing more detailed rules regarding the content of the policy, in accordance with the purpose and aim of this policy;
- Communicating details about the policy and its underlying governing documents to ensure good knowledge about them among employees;
- Monitoring compliance with the policy and its underlying governing documents in a satisfactory manner;
- Where applicable, ensuring in the event of irregularities or serious deviations from the policy the taking of legal or disciplinary action, or assisting with this; and
- Taking the corrective actions and performing the reporting necessary to fulfil the purpose and intent of the policy.

Each respective Head of is ultimately responsible for creating awareness of the policy and for monitoring compliance in their particular business area. The respective Head of Corporate Functions has the corresponding responsibility.

All Grant Thornton employees are expected to comply with the adopted policy and to inform their immediate manager or the policy owner of any non-conformities relating to the policy. Alternatively, it is possible to submit reports via our whistleblowing function.

7. References

The policy is supplemented by underlying instructions that contain more detailed rules regarding information security and data protection.

8. Version history

Version	Date	Comment
1.0	15/01/2024	First version of the policy.
1.1	22/11/2024	Annual review and minor updates.
1.2	24/11/2025	Annual review; new section 5.3.1 on the responsible use of digital tools and services, as well as minor editorial changes in other places.
2.0	25/08/2026	Update relating to legal structuring of operations