Data Protection and Cyber Security

Our approach

Data protection and cyber security are essential to Storskogen's ability to operate responsibly, safeguard trust, and create long-term value.

Storskogen operates through a decentralized business model. Rather than centralising systems, the focus is on ensuring that risks are effectively managed at subsidiary level, supported by clear group-wide expectations, governance, and follow-up.

Our approach is risk-based and proportionate. Each subsidiary prioritises actions based on size, operations, and exposure, while ensuring that fundamental controls are in place. Data protection and cyber security are treated as core business risks.

Governance

Responsibility lies with each subsidiary's management team and board. At Group level, oversight is integrated into the overall governance framework, including Audit Committee oversight.

Relevant matters are reported to Group management and, where material, to the Audit Committee.

Storskogen has established group-level policies covering data protection and information security, including a Privacy Policy and supporting internal guidelines. These policies define how personal data is collected, used, stored, and protected, set requirements for subsidiaries and third-party service providers, and, where relevant, are expected to be reflected in supplier and IT service provider arrangements.

The policies also address data subject rights, including access, correction and deletion of personal data, as well as principles for data retention and handling of related requests.

These policies are supported by operational processes, including regular risk assessments (where relevant including data protection impact assessments), incident management procedures, and employee awareness and regular training.

At Group level, material risks and incidents are followed up on a regular basis to support oversight and continuous improvement.

Group-wide expectations include:

- Adoption of data protection and information security policies
- Clear roles and responsibilities at management level
- Ownership of business-critical systems and data

- Compliance with applicable laws, including GDPR
- Integration into risk management and internal controls

Risk management and controls

Subsidiaries identify and manage risks as part of regular risk processes. Risk assessments are conducted regularly and used to prioritise actions.

Core elements include:

- Identification and assessment of cyber security and data protection risks
- Classification of information based on sensitivity and business impact
- Implementation of appropriate technical and organisational safeguards, such as access control and secure handling of information
- Management of risks related to third-party suppliers and external IT services
- Periodic review of key controls and processes to ensure effectiveness

Implementation across the portfolio

Implementation is adapted to each company's size and maturity:

- Smaller companies focus on basic controls and external IT expertise
- More mature companies apply structured governance, monitoring and dedicated resources

Employees are expected to maintain awareness of relevant risks. Training and internal communication are used to support this, with training provided on a regular basis where relevant.

Incident management and follow-up

Subsidiaries maintain procedures for identifying, reporting and managing incidents.

This includes:

- Internal reporting and escalation routines
- Mitigation and recovery actions
- Root cause analysis and corrective actions

Personal data breaches are handled in accordance with applicable legislation, including notification requirements.

Continuous improvement

Storskogen continuously strengthens its approach through:

- Regular risk reviews
- Integration into governance and reporting
- Support to subsidiaries based on business risk

The ambition is to manage data protection and cyber security as an integral part of business resilience and long-term value creation.

Key indicators and proof points

To support transparency and demonstrate implementation, Storskogen monitors and follows up key indicators across the portfolio. These include:

- Subsidiaries conduct regular risk assessments related to cyber security and data protection
- Defined procedures for incident reporting, escalation and breach notification
- Employees receive relevant awareness and training based on their roles
- Management-level accountability for data protection and cyber security
- Regular follow-up of material risks at Group level
- Requirements for third-party suppliers and IT service providers

These elements support continuous improvement and ensure that risks are managed in line with business impact and regulatory expectations.