Title	Version	Replaces	Org. location	Page # (of #)
Policy for Information and Data	1.5	1.4	N/A	1(3)

Owner	Changed by	Latest changed	Document type
CFO	Anna Forsebäck	2026-04-14	Policy

Adopted by	Adopted on (Date)	Status	Replaced by
The Board of Directors	2026-05-08	Adopted	N/A

Policy for Information and Data

Background

What does this policy include?

This policy applies to Hemnet Group AB (publ) and its subsidiaries ("Hemnet") and covers all handling of information and data within the business.

Who is affected by this policy?

This policy primarily concerns employees involved in collaboration for information and data governance.

Why have we created this policy?

The purpose of this policy is to establish an approach to information and data that promotes innovation and a high pace in product and business development, while simultaneously protecting assets and ensuring compliance through continuous, risk-based efforts. The policy sets the direction, approach, and overall framework for the collaboration that takes place within the scope of 'data governance'.

Definition

Data refers to raw material in the form of individual values, numbers, or unprocessed facts. Information refers to data that has been placed in a context and given a meaning. Both data and information may consist of personal data. These definitions encompass all data and information handled within Hemnet, regardless of format, storage location, or the system in which it is processed.

Data Governance and Overall Objectives

Information and data constitute some of Hemnet’s most valuable assets and are fundamental to innovation, as well as to driving and developing the business—for example, through data-driven decision-making. A forward-leaning approach to technological development and AI is central to strengthening competitiveness and creating the greatest possible value for Hemnet. At the same time, AI and technological progress mean that the Company’s exposure to cyberattacks is increasing, and the regulatory landscape is complex.

Against this background, it is essential to have a data governance model that considers the balance between promoting innovation and implementing risk-mitigating measures. The objective of Hemnet’s information and data governance is to achieve frictionless, lawful, secure, and quality-assured handling that meets the needs of the business. This governance enables innovation while ensuring that individual privacy is consistently respected.

Hemnet's data governance is established through a collaborative model where security and speed reinforce one another. Through active and structured collaboration for data governance, we create the conditions for high mobility and operational pace, while simultaneously supporting the integration of information security, data protection, and AI governance.

Principles for Data Governance

Hemnet's data governance forms the foundation of the Company's work with information security, data protection, and AI. The following principles define how responsible handling is combined with value-creating innovation.

Data Quality and Responsibility
Hemnet shall strive to ensure that the data assets most valuable to the Company are accurate, reliable, and complete throughout their lifecycle. It shall be an integral part of the Company's collaborative model for data governance to establish ownership of data quality.

Protective Measures
Information security efforts shall be based on international standards, such as ISO 27001 and ISO 27701, but are conducted using a risk-based and proactive approach to ensure that Hemnet's protective measures act as a direct enabler for innovation and value creation.

Hemnet shall apply protective measures that are proportionate to the identified risks and the needs of the business. This encompasses Hemnet's own environment as well as instances where information and data are handled by external parties and suppliers. By balancing security against business value, assets are protected in a way that minimizes uncertainty and creates the security required to maintain a high pace of innovation and operational speed.

GDPR Compliance and Personal Privacy
Hemnet shall maintain a risk-based compliance approach characterized by respect for personal privacy, contributing to the Company's reputation and the trust of our customers and users.

Incident Management and Continuity
Hemnet shall work in a structured manner to quickly detect, manage, and follow up on incidents, which is crucial for limiting any potential damage. Lessons learned from occurred incidents shall be used proactively to strengthen protection and reduce the risk of similar events recurring. Furthermore, Hemnet shall ensure robust continuity planning so that critical functions and data can be maintained and restored with minimal delay, increasing the organization's resilience against disruptions, attacks, and outages.

A Culture of High Awareness
Hemnet shall promote a culture of high awareness regarding information security, data protection, and AI, and engage in proactive efforts aimed at making it easier for employees to follow applicable guidelines and instructions.

Governance

Roles and Responsibilities

This policy is owned by the CFO, and any updates or amendments require approval from the Board of Directors. Management and the Board are responsible for ensuring that data protection and information security are maintained in accordance with this policy. To ensure that Hemnet's use of information and data is aligned with business objectives, management shall also be responsible for maintaining clear governance over Hemnet's strategic decisions and investments. This includes ensuring that roles, responsibilities, and authorities are clearly documented. All individuals with access to Hemnet's resources must comply with this policy and report any breaches.

Follow-up and compliance

Monitoring and Review

This Policy shall undergo an annual review in accordance with Guidelines for Hemnet's Governing Documents and Policy for Corporate Governance, in order to ensure that it is correctly formulated and remains fit for purpose for the Company's operations. The review is conducted by HOIS (Head of Information Security) and aims to assess whether the Policy needs to be updated as a result of changes in applicable regulations, the Company's operations or working methods, or whether there is otherwise a need for clarification to ensure that the Policy provides appropriate and clear support for regulatory compliance and good corporate governance. The review is conducted as part of the Company's overall work on risk management and corporate governance.

Policy Accessibility

This policy is accessible to all employees and relevant stakeholders through internal communication platforms and Hemnet's corporate website at https://www.hemnetgroup.se/. Educational initiatives and supporting materials are provided to ensure that Hemnet's requirements for information and data handling are complied with throughout the organisation.

Reporting channels for compliance issues

Hemnet's Code of Conduct indicates which reporting channels are to be used by employees who detect violations in compliance with Hemnet's steering documents. Each employee is asked to raise compliance issues with the person concerned in the matter in the first place where possible. If it is not suitable or possible, the employee should contact the immediate supervisor. If that is also not suitable or possible, employees are asked to contact their supervisor's supervisor, Hemnet's Chief People & Culture Officer or Hemnet's General Counsel. Also, severe misconduct can be reported anonymously via the Company's whistleblower function available via https://report.whistleb.com/en/hemnet.

Violations of this policy

Breaches of this policy are taken seriously and may be addressed through appropriate measures, which in some cases could include disciplinary action. If a breach also involves a violation of applicable laws, it may have legal implications for both you as an individual and the Company.

Related documents

- Code of Conduct
- Guidelines for Data Protection
- Guidelines for information security
- AI Guidelines