Atea ASA

Data Protection Policy

Atea ASA and its business units (hereinafter referred to as Atea), is the market leader in information technology infrastructure and related services for businesses and public-sector organizations in the Nordic and Baltic regions. Atea is committed to protecting personal data to respect the fundamental rights and freedoms of individuals. As a controller and processor of personal data, Atea must ensure an adequate level of protection when processing data about employees, customers, partners, and suppliers.

Purpose

The purpose of this policy is to set the standard for the protection and processing of personal data within Atea and its business units. Corporate management is committed to ensuring compliance with applicable data protection laws and regulations.

Scope

This policy applies to Atea and its entire operations including employees, customers and suppliers and covers all data related to individuals processed by Atea and its business units. Country-specific laws and regulations must be addressed in business unit-specific policies, if applicable.

In case of breach of this Policy, corrective and disciplinary actions must be initiated as defined in Atea Code of Conduct

Definition

The General Data Protection Regulation (“GDPR”) is an EU regulation that outlines how organizations shall process and protect personal data.

The key principles of GDPR includes lawful, fair, and transparent processing of personal data, ensuring that individuals’ rights are respected, data is kept secure, updated and for a limited period, and ensuring security and accountability for the processing of personal data.

Personal Data Protection, covered by Information Security, applies to all personal data, regardless of the technology or storing methods.

Personal Data Protection is a way to achieve data privacy and is covered by Information security since the technical and organizational measures apply to all information.

Objectives

Atea’s objectives of personal data processing are to support the business strategy by:

- Complying with applicable laws by implementing appropriate organizational and technical measures to protect personal data using a risk-based approach. Organizational and technical measures must ensure confidentiality, integrity, and availability in accordance with Atea Information Security Policy (ATEAIS-P001).
- Governing Data Processing Agreements (DPAs) when processing activities are performed where Atea is acting as a Controller or a Processor.
- Achieving maturity of employee behavior for personal data protection through appropriate awareness training.
- Preventing or minimizing the impact of personal data breaches.
- Ensuring that every employee understands responsibility for handling personal data correctly.

Execution

When protecting personal data, Atea shall consider risks to data subjects' rights and freedoms, the business, and costs of the safeguards. Based on the considered risks, technical and operational measures must be taken in a well-planned manner with sufficient follow-up to achieve compliance with GDPR.

Management system of data protection

The Privacy Information Management System (PIMS) is defined by the ISO/IEC 27701 standard for privacy, as well as information security management system (ISMS) based on the ISO/IEC 27001 standard which states the level of security and process controls for the right level of data protection for Atea.

Atea has integrated the PIMS into its group-wide risk management, which forms part of Atea's ISMS and is described in the Information Security Policy.

Business units may have local supporting documentation for data protection aligned with Atea Group governing documentation.

An annual plan for data protection must be prepared, based on an analysis of new laws or regulations, risks or other requirements.

Atea conducts an internal audit of Privacy annually across all business units. Regular privacy audits are essential for ensuring compliance with GDPR regulations and protecting personal data.

Roles and responsibilities

- The CEO of Atea ASA is ultimately responsible for the protection of personal data, with responsibility delegated to the COO, who has the right to approve this policy.
- Business unit responsibility is delegated to the local Business unit CFO.
- Atea Group personal data protection management responsibility is delegated to the Group CISO, who has the right to approve topic-specific policies and other GDPR documentation.
- Group Privacy Officer leads the data protection work in Atea and coordinates Business Units DPO activities.
- Business Unit Data Protection Officers are responsible for local operations.
- Each person responsible for a business area must ensure compliance with this policy and underlying governing documents.
- Each employee is responsible for handling personal data correctly and securely.

Published June 2026