Information Security and Data Protection Policy

We take care of our own and our customers' data security and the implementation of data protection. In the information security requirements, we take into account the actual needs of the operation as well as the relevant regulations and the requirements of the ISO 27001 standard.

The purpose of the information security arrangements is to secure the information and its processing and to manage the related risks. Our target is zero Information security breaches. Data is processed in compliance with legislation and in accordance with good data management and processing practices. Information security arrangements aim to ensure that information and information systems are reliable and accessible to authorized users. Only individuals and entities with the proper authorization may handle data, and only to the extent required by their work tasks. Events related to data processing must be traceable to the necessary extent.

Data security and data protection goals, principles and requirements apply to all personnel. Our entire staff is committed to these principles, and we expect the same from our partners. Data security requirements must be taken into account when developing operations and systems and planning finances. Every employee must know the information security risks related to their own tasks and the measures required to manage them, and act accordingly. Our target is that every employee within Algol Group performs our internal Information security education.

Risks are systematically assessed and managed to reduce them to an acceptable level. The same requirements, as well as any separately agreed-upon requirements, also apply to those performing tasks on behalf of or under contract with the organization who handle or have access to data under the organization's control. All agreements must adequately consider the obligations of this information security and data protection policy.

Public | Version 2.1 | Approved 1.4.2025 / Revised 2.7.2026

We monitor the realization of our operations and goals regularly, and the goal is to continuously improve operations. Each person is responsible for the information security of their own task area. The CEO has the ultimate responsibility. The information security officer is responsible for the coordination and general development of information security issues.

The implementation of goals and principles is monitored administratively and technically. Circumventing, breaching, or attempting to breach information security arrangements is prohibited and punishable. Any identified deficiencies, misuse, or other issues compromising information security must be reported.

The Information security and data protection policy is evaluated by Algol Group Sustainability Manager on a yearly basis.

April 2025,

Joakim Flinck
CEO of the Algol Group