






Elmos ESG Policies

Section:	Governance
Chapter:	Information security
Policy:	Information security and data protection
Coverage:	Elmos Group
Supported UN SDGs:	  
Addressed GRI Standards:	2-27, 418

Introduction: Elmos has a Compliance Management System (CMS). The Elmos CMS represents a binding Group-wide framework for all employees for the purpose of complying with applicable laws, regulatory provisions and internal and external rules and regulations in all business areas. The topics of information security and data protection are also covered by the Elmos CMS.

Information security: Information are one of a company's most valuable assets. Therefore, all information - analog and digital - must be protected. Elmos ensures that only authorized people have access to such sensitive information and that unauthorized or uncontrollable access or distribution cannot take place. We are guided by the three most important objectives of information security C - I - A (Confidentiality, Integrity, Availability) and have established a corresponding Information Security Management System (ISMS).

TISAX (Trusted Information Security Assessment Exchange) is a standard derived from ISO 27001 that regulates the exchange of assessment results in accordance with the VDA-ISA standard specific to the automotive industry. Topics include the classification of information, the confidentiality of information (including intellectual property), security zones, our security personnel and cyber security. Elmos has successfully passed an assessment in accordance with TISAX Level 3. As an innovative company, we also hold regular discussions with potential business partners. Here, too, we place the highest value on information security and data protection. We therefore conclude numerous contracts for commissioned data processing and non-disclosure agreements every year.

Data protection: The prohibition of the processing of personal data is laid down as a basic principle in the General Data Protection Regulation (GDPR). Elmos fully complies with the GDPR and only agrees to data processing or use of personal data if it is either permitted by law or authorized by the data subjects.

Of course, Elmos respects all data subject rights. Corresponding process descriptions for data disclosure and/or data deletion are set out in our Privacy Policy, for example. It represents the company-wide set of rules for implementing data protection in accordance with the GDPR. It therefore constitutes the code of conduct for processing personal data for all Elmos employees. The Privacy Policy can be found on our website and on the company intranet. The intranet also contains an FAQ¹ on data protection and the GDPR.

Responsibilities: Overall responsibility lies with the Management Board. Responsibility for information security lies with our Chief Information Security Officer (CISO). Responsibility for data protection lies with our Data Protection Officer. For example, this officer maintains the register of processing activities relating to personal data required by the GDPR. Both the Information Security Officer and the Data Protection Officer report regularly and as required, but at least once a year, to the Management Board and Supervisory Board on the topic of IT security. In addition, our Works Council (due to its right of participation) or our IT

¹ Frequently Asked Questions

department (for example in the case of software and hardware integration) may be involved in selected issues relating to data protection.

In the event of security incidents affecting Elmos IT, the Computer Emergency Response Team (CERT) must also be informed, which will immediately define and initiate the next steps. In the event of a data breach, there is an internal reporting obligation. Corresponding reports can be made via a form on the intranet. The data protection officer will review the incident and initiate any necessary measures.

Training: All employees must attend mandatory training on the topic of “Cyber Security” and mandatory training on the topic of the “Information Security Management System” once a year. In addition, all employees must take part in mandatory training on data protection every two years. As part of the training, presentations must be worked through and effectiveness tests must be passed. In addition to definitions of terms and legal frameworks such as the GDPR, the content also includes case studies on cyber security and instructions on remote working and how to use video conferencing. In addition to the mandatory training, Elmos conducts company-wide phishing tests several times a year to raise employee awareness.

ESG policies	Business ethics and anti-corruption Compliance management system (CMS) Quality and crisis management
ESG KPIs	Average hours of training
Certificates	Quality Management System Certificate IATF 16949:2016
Accompanying documents	Code of Conduct for Employees Code of Conduct for Suppliers and Business Partners
Additional documents	Privacy Policy
