INFORMATION SECURITY AND DATA PROTECTION POLICY

Cod. **PO-ISMS.01.EN** Rev. **00** del **05/11/2023**
Type: **General Policy**
Classification: **L1 – PUBLIC**

CONTROLS REFERENCES
VDA/ISA 5.1.0: C.1.1.1
ISO 27001:2022: A.5.1
REGULATION (EU) 679/2026

MATRIX OF REVISION

Rev.	Date	Description	Drafted	Verified	Approved
0	06/11/2023	First issue in the ISMS	RSI + CPD	QM	AD

REGULATORY REFERENCES

Titolo	Note
VDA/ISA 5.1.0	VDA Information Security Assessment Ver. 5.1.0
ISO/IEC 27001:2022	Information security, cybersecurity and privacy protection — Information security management systems — Requirements
Regulation EU 2016/679	General Data Protection Regulation (GDPR)

1 FOREWORD

SPESSO GASKETS s.r.l. is a company specializing in the design and production of gaskets. The company attaches primary importance to information security, especially in an environment characterized by constant technological evolution and incessant data protection challenges. Offering solutions to original equipment manufacturers (OEMs) and the aftermarket, the company is fully aware that the trust placed in it by its customers and partners lies not only in the quality of the products supplied, but also in the ability to ensure the integrity, confidentiality and availability of the information handled.

2 SCOPE

The objective of this policy is to ensure the protection of corporate information handled in the design, production, and development of braking systems for the automotive industry against all threats, whether internal or external, intentional or accidental.

3 APPLICATION

This policy applies to all personnel, both internal and external (e.g., suppliers), involved in the processes of designing, manufacturing, and developing our products, as well as to services, technical resources, infrastructures, and business processes involved, even indirectly, in the design, manufacturing, and marketing of such products.
The scope of application includes both corporate information and information processed on behalf of our customers, regardless of their nature or form (digital, paper, verbal, etc.).
The policy applies to all places, activities, and processes in which design, manufacturing, or support activities are carried out.
All employees, collaborators, and suppliers involved in the activities of designing, manufacturing, and marketing products are required to apply this policy and to contribute to its implementation and to the achievement of the information security objectives set forth therein.

4 DEFINITION OF INFORMATION SECURITY

For SPESSO GASKETS, information security means safeguarding information and the associated information systems against unauthorized access, misuse, inadvertent disclosure, disruption, alteration, or destruction.

5 OBJECTIVES

The primary objective is to ensure the security of processed information, continually guaranteeing the following properties of the information:

- **Confidentiality**: ensuring that information is accessible only to those who are authorized to access it.
- **Integrity:** maintaining the accuracy and completeness of the information and its processing.
- **Availability:** ensuring that authorized users can access the information and relevant resources when needed. SPESSO GASKETS also has the following additional objectives:

5.1 INFORMATION SECURITY.

- **Technological Assets:** Preserve the security of technological assets that support information processing;
- **Compliance and Legality:** Ensure and guarantee compliance with laws, regulations, and contractual obligations;
- **Business Continuity:** Ensure the continuity of business operations in the event of security incidents;
- **Personnel:** Promote awareness of information security among employees and external stakeholders.
- **Corporate Services:** Ensure the reliability and security of all components supporting corporate services;
- **Communications:** Ensure the security of the channels through which information is transferred;
- **Risk:** Manage and control information security risks, keeping them within acceptable levels;
- **Certifications:** Assure customers and other stakeholders of our ongoing commitment to protecting their information through the achievement of specific certifications (e.g., TISAX);
- **Collaboration:** Support clients in managing security risks, both in formal/documentary activities and in substantive activities related to risk prevention;
- **Design and Development:** Develop business processes based on recognized standards, established methodologies, contractual obligations, laws, and applicable regulations.

5.2 PERSONAL DATA PROTECTION

- **Awareness and Training:** Ensure that all employees are aware of the GDPR requirements and are adequately trained to properly handle personal data.
- **Design and Privacy by Default:** Integrate privacy from the early design stages of products and services, adopting suitable technical and organizational measures to ensure the protection of personal data.
- **Data Protection Officer (DPO):** Regularly assess the conditions for mandatory appointment as established by Article 37 of the EU Regulation 2016/679 and, if necessary, appoint a Data Protection Officer (DPO).
- **Informed Consent:** Obtain explicit and informed consent from the data subjects before collecting or processing their personal data, providing clear and transparent information on the purposes and methods of processing.
- **International Data Transfers:** Ensure that transfers of personal data outside the European Economic Area (EEA) are conducted in accordance with GDPR provisions, for example, using standard contractual clauses or certification mechanisms.
- **Protection of data relating to criminal convictions and offences and special categories of personal data :** Process data relating to criminal convictions and offences and special categories of personal data in compliance with the restrictions set by the GDPR, adopting adequate security measures to prevent unauthorized access, disclosure, or use of such data.

- **Rights of Data Subjects:** Respect and facilitate the exercise of the rights of data subjects, such as the right to access, right to rectification, right to erasure (right to be forgotten), right to data portability, and the right to object to processing.
- **Data Security:** Implement adequate security measures to protect personal data from loss, unauthorized access, alteration, or illicit disclosure, considering the state of the art, implementation costs, and the nature, scope, context, and purposes of processing.
- **Data Protection Impact Assessment (DPIA):** Carry out Data Protection Impact Assessments (DPIAs) when necessary to assess and mitigate the risks associated with personal data processing activities, especially when the processing could pose high risks to the rights and freedoms of individuals.
- **Data Breach Notification:** Promptly notify any personal data breaches to the competent supervisory authorities and, if applicable, to the data subjects, in accordance with GDPR's notification requirements.
- **Data Retention:** Retain personal data only for as long as necessary to fulfill the purposes for which it was collected, respecting the legal retention limits and ensuring that the data is securely deleted after the retention period has elapsed.
- **Privacy in Marketing Communications:** Comply with GDPR norms for marketing activities, such as obtaining consent from data subjects for sending marketing communications and providing them with the option to withdraw consent at any time.
- **Service Provider Accountability:** Ensure that service providers processing personal data on behalf of the company are appropriately selected, evaluated, and bound by contractual agreements that establish GDPR compliance obligations.
- **Monitoring and Auditing:** Implement internal monitoring and auditing mechanisms to ensure GDPR compliance, identify potential violations, and take appropriate corrective actions.
- **Awareness of Privacy Rights of Data Subjects:** Inform data subjects about their privacy rights, provide clear information on the handling of their personal data, and respond to their requests and concerns promptly and effectively.

6 STRATEGY

To achieve objectives, the following operational strategies are adopted:

- Always operate in compliance with contractual and regulatory agreements;
- Promote the professional development and professionalism of our collaborators through continuous training and updating activities;
- Ensure that all activities are carried out with seriousness, competence, and professionalism;
- Implement an integrated management system for information security and personal data protection, based on the ISO/IEC 27001:2002 guidelines, capable of providing tools and control processes to constantly improve methods and results;
- Involve and sensitize staff to operate in accordance with this policy and to act in compliance with the requirements established by the management system and to report any information security breaches they become aware of.

7 INFORMATION SECURITY MANAGEMENT SYSTEM REQUIREMENTS

The integrated management system for information security and personal data protection meets the following minimum requirements:

- Constant monitoring of processes and information security measures;
- Prompt registration, analysis, and investigation of any non-conformities, violations, and security incidents, identifying causes and defining appropriate mitigation actions;
- Conduct of internal audits and audits by independent bodies to verify the effectiveness of information security controls and countermeasures;
- Optimal allocation of investments based on the type of information processed and the security needs expressed by stakeholders;
- Provision of adequate training to staff and dissemination of the culture of information security.

8 PRINCIPLES RELATING TO INFORMATION SECURITY AND DATA PROTECTION MANAGEMNT SYSTEM

The guiding principles for all information security and data protection activities are as follows:

- **Classification and Protection:** All information is a valuable asset and must be classified according to its sensitivity and adequately protected according to its criticality;
- **Access to Information:** Access to information must be based on the 'need-to-know' principle and controlled on the basis of a specific access control policy.
- **Security measures:** Security measures must be proportional to the risk.
- **Encryption:** The most sensitive information must be encrypted during transmission and when stored on portable devices or external systems.
- **Integrity of Information**: Measures must be taken to ensure the integrity of the information.
- **Retention of Information:** Information must be retained for the period required by law or internal company policy.
- **Destruction of Information:** Information must be securely destroyed when it is no longer needed.

9 COMMITMENT TO MEET APPLICABLE REQUIREMENTS

SPESSO GASKETS is committed to complying with all laws, regulations and other requirements applicable to information security and data protection. This includes, but is not limited to, the protection of personal data, intellectual property, libel laws, criminal law and contracts with customers and suppliers and other interested parties.

10 RESPONSABILITY

Everyone directly or indirectly involved in the design and production of gaskets is responsible for understanding and adhering to this policy, and for reporting any violations or potential information security risks.

11 SANCTIONS

Failure to comply with the information security and personal data protection requirements established by this policy or the integrated management system may result in disciplinary sanctions, up to the termination of the employment or contractual relationship.

12 MANAGEMENT COMMITMENT

The management is committed to continuously improving the integrated management system for information security and personal data protection through regular review of policies, controls, the effectiveness of security measures, and compliance with applicable laws and regulations.

13 MANAGEMENT OF EXEMPTIONS AND EXCEPTIONS

Exemptions and exceptions to the this policy are allowed, upon approval of the general management, only in extraordinary and extremely necessary cases. Exceptions must be adequately documented and regularly reviewed to ensure that they are still necessary.

14 COMPLIANCE

This policy is consistently maintained in line with applicable legislative, regulatory, and contractual requirements.

15 V VALIDITY APPROVAL AND AMENDMENTS

This policy for information security is approved by the General Management. All changes to this policy must be approved by the General Management before implementation.
The policy is valid from the date of approval.

Torino, 06/11/2023
Chief Executive Officer
Gabriele Orsucci