AI GOVERNANCE - AI POLICY

APPROVED BY

PRYSMIAN S.p.A BOARD OF DIRECTORS

OCTOBER 29th, 2025

The planet’s pathways

TABLE OF CONTENTS

1. PURPOSE

Prysmian recognizes the transformative potential of Artificial Intelligence (AI) to enhance operations, products, and services. This Policy outlines Prysmian's commitment to responsible AI use to ensure ethical considerations are upheld, AI risks are managed, and compliance to applicable regulations is achieved. The document provides a framework to guide all AI-related activities, offering guidelines for informed and responsible use of AI, and establishing principles, instructions, and rules on acceptable and unacceptable behaviors.

2. SCOPE

This policy applies to all Prysmian Group entities (here in after the "Group"), including third parties.

3. AUDIENCE

This policy applies to all personnel, both internal and external, involved in managing or using the Group's AI assets (including online/cloud systems). It covers all AI systems developed or used by the Group within its area of responsibility.

4. DEFINITIONS

AI system - Means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

AI Types – Traditional AI, Generative AI, Agentic AI

Algorithm – A series of mathematical instructions used by AI systems to process data and make decisions.

Bias – Distortion in data or algorithms that can lead to incorrect or discriminatory decisions.

Intellectual Property – The set of legal rights that protect creations of the human mind, such as inventions, literary and artistic works, designs, symbols, names, and images used in commerce.

Biometric categorization - Process by which an AI system analyzes biometric data—such as facial features, fingerprints, voice patterns, or other physiological and behavioral characteristics—to classify individuals into specific categories based on predefined attributes (e.g., age group, gender, or ethnicity).

Deep Learning – A Machine Learning approach based on deep neural networks for recognizing complex patterns in data.

Inference – The process by which an AI model applies what it has learned to generate predictions or decisions on new data.

Hallucinations - Instances where an AI model generates incorrect, misleading, or entirely fabricated outputs that are not based on the input data or real-world facts

Machine Learning – A subset of AI that uses algorithms to learn from data and improve performance without being explicitly programmed.

Model - Concrete implementation of an algorithm trained on a specific dataset. After an algorithm processes the data and optimizes its parameters, the result is a model that can be used to make predictions, decisions or conduct actions.

Neural networks - Computational model that consists in layers of interconnected nodes (neurons) that transform inputs through weighted connections and activation functions

5. REFERENCES

Internal references:

1. Prysmian’s Code of Ethics
2. Code of Business Conduct
3. Cryptography Policy - PO-HR&O-SEC-013
4. Data Classification Policy - PO-HR&O-SEC-010
5. Data Breach Incident Management - OP-HR&O-SEC-006

External references:

1. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (so-called ‘EU AI ACT’ - link]
2. Italian Law No. 132/2025, governing the development, adoption, and governance of AI systems [link]
3. ISO/IEC 42001:2023 - Information technology — Artificial intelligence — Management system.
4. ISO/IEC 23894:2023 - Information technology — Artificial intelligence — Guidance on risk management.
5. NIST AI 100-1 - Artificial Intelligence Risk Management Framework (AI RMF 1.0).

6. GENERAL PRINCIPLES

AI DEFINITION AND TAXONOMY

According to the EU AI ACT, an AI system is defined as a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

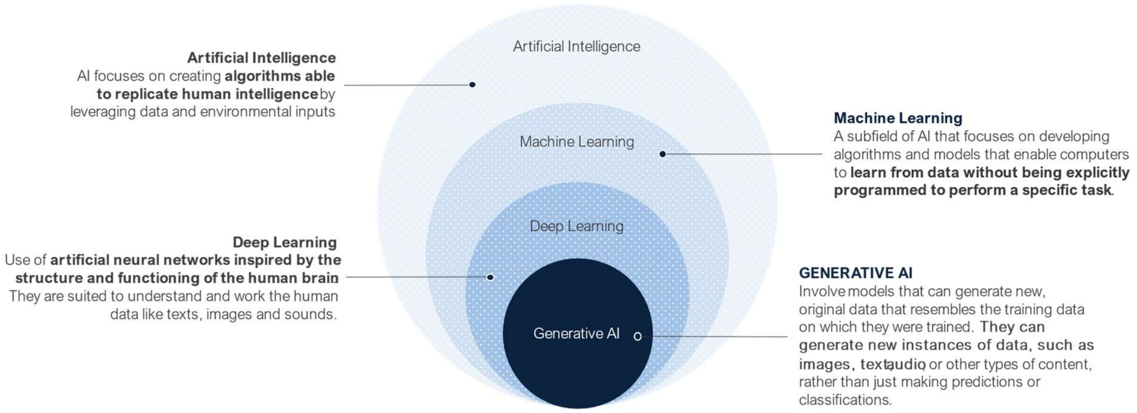

Artificial Intelligence
Machine Learning
Deep Learning
Generative AI
Artificial Intelligence
AI focuses on creating algorithms able to replicate human intelligenceby leveraging data and environmental inputs
Machine Learning
A subfield of AI that focuses on developing algorithms and models that enable computers to learn from data without being explicitly programmed to perform a specific task.
Deep Learning
Use of artificial neural networks inspired by the structure and functioning of the human brain They are suited to understand and work the human data like texts, images and sounds.
GENERATIVE AI
Involve models that can generate new, original data that resembles the training data on which they were trained. They can generate new instances of data, such as images, text,audio, or other types of content, rather than just making predictions or classifications.

Figure 1: Hierarchical relationship among different areas of AI: Artificial Intelligence (AI), Machine Learning, Deep Learning, Generative AI, and Agentic AI.

Machine Learning & Deep Learning

Machine Learning and Deep Learning rely on predefined algorithms and models that allow computers to learn from data, often through the analysis of existing datasets and patterns, even without being explicitly programmed to perform specific tasks. They do not create new content but focus on optimizing processes and decision-making based on information.

Machine Learning and Deep Learning are used in the Energy and Telecommunication sector for various purposes, including:

- Predictive maintenance of systems:

  Neural networks analyse IoT data from turbines, solar panels, and power plants to detect anomalies and prevent failures.

Machine Learning and Deep Learning offer efficient solutions for data analysis, operational optimization, and decision-making support across various sectors.

Generative AI

Generative Artificial Intelligence (Gen AI) is a branch of AI that focuses on creating new content or data from existing inputs. Unlike traditional forms of AI, which primarily rely on data classification and analysis, Gen AI can produce original outputs in various formats, such as text, images, audio, and video, in response to user prompts (inputs).

Generative AI takes different forms and is used, for example, to:

- Chatbots

  Leveraging generative language models to develop chatbots that provide accurate and detailed answers based on an official internal document corpus, including company policies, operational procedures, technical instructions, and software user manuals.
- Agentic AI

  Agentic AI operates through Large Action Models (LAMs) or similar architectures that integrate perception, reasoning, and execution capabilities. These systems can plan multi-step activities, interact with other agents or humans, and adapt their strategies based on feedback and context.

Generative AI offers new ways for users to efficiently create, summarize, edit, and perform tasks involving content production.

Adoption of AI Systems

The adoption of AI systems undoubtedly brings significant advantages, such as increased efficiency, automation, and data processing capabilities. However, to maximize these benefits, it is crucial to carefully assess the associated risks, including the potential for erroneous decisions, reduced transparency in decision-making processes, and ethical implications of data use. These risks also include possible impacts on Prysmian's operations, compliance with current regulations, and the company's reputation.

RISKS AND CHALLENGES OF AI

It is important to recognize that the use of artificial intelligence technologies can expose Prysmian to multiple challenges and risks. Some of the main risks, aligned with the NIST AIRMF (Artificial Intelligence Risk Management Framework) standard, are listed below.

- Data Privacy and Security

Artificial intelligence systems are generally based on "black box" models trained on vast datasets available from numerous sources, which makes it complex to clearly trace the origin and use policies of the data. Moreover, the sharing of confidential information during the training or operation of an AI system could lead to the release of such information to unauthorized parties. Finally, the collection of customer and employee input raises several concerns regarding the rights to use such data for training models.

In this context, it is crucial to take privacy and data protection regulations into account. In particular, any processing of personal data performed by or in connection with AI systems must comply with the principles and obligations set out in the GDPR, including but not limited to lawfulness, fairness, transparency, purpose limitation, data minimization, integrity, confidentiality, and accountability. In addition, the use of AI systems and any related data processing activities must adhere to the provisions of the applicable Company policies, including those governing privacy governance and the use of corporate tools.

Example: Training AI systems with confidential business information or personal data for purposes other than those indicated in the information notices provided to Prysmian employees , may entail the risk of exposing such information to unauthorized users through specific requests or queries.

- Intellectual Property

There is a risk that GenAI may generate content based on pre-existing material that is protected by intellectual property, thus infringing copyrights or patents.

Furthermore, it is not always clear who the actual author of the content generated by GenAI systems is - for example, it could be argued that the author of the output of an AI system is the author of the prompt from which it was generated or, conversely, the company developing the AI system.

Example: Using images generated by tools that do not guarantee training on copyright-free data in documents that will be made public, with the risk of copyright infringement.

- Bias

The data used to train the model may not be fully representative and may be biased towards certain groups of individuals. This could generate and amplify discrimination in the results generated, possibly perpetuating negative effects on end users.

Example: Excluding the CVs of female candidates, fuelling a gender bias and making it more difficult for women to enter the company, even though they may have appropriate qualifications and skills.

- Accuracy and Reliability

AI systems may produce errors during use. Artificial intelligence can sometimes produce inaccurate or unrealistic content, or even generate hallucinations, where results may appear consistent but lack a basis of veracity. The quality of responses generated by artificial intelligence must be verified before they are used.

Example: An inaccurate demand forecast could lead to overproduction, increasing storage costs, or underproduction, resulting in delays in customer deliveries.

- Compliance to regulations and Accountability

The EU AI ACT, the first artificial intelligence regulation, was passed in March 2024 and came into force in August 2024. The risk of non-compliance with the EU AI ACT can lead to significant consequences for the organisation, including legal sanctions and reputational damage.

Example: The development or use of an artificial intelligence system that falls under the prohibited purposes defined by the regulation may result in financial penalties for the company.

Moreover, the Italian Law No. 132/2025, was passed on 25 September 2025 and came into force on 10 October 2025. This law establishes the national framework for the development, adoption, and governance of AI systems, in line with the European EU AI ACT. The risk of non-compliance with the Italian AI Law may lead to further legal risks and reputational damage for the organisation.

Example: The use of AI systems in employment processes without providing workers with the required information, as mandated by Article 11 of the law, may lead to compliance violations and reputational risks for the Company.

- Sustainability

The training of AI models requires the use of huge amounts of computational resources, as machine learning processes are highly complex and require intensive processing to analyse and handle large volumes of data. This significant use of computing power leads to high energy consumption, which not only affects the operating costs of IT infrastructures, but also has a considerable environmental impact. Indeed, the high energy requirements associated with these operations contribute to increased carbon emissions and pressure on natural resources, raising important sustainability issues in the development and implementation of AI technologies.

Example: The use of high-performance servers, cloud computing, or data centres that consume a significant amount of energy and contribute to carbon emissions.

- Transparency and Explainability

The lack of transparency in AI systems could lead users to misinterpret the information received from the system, as well as how personal and non personal data are processed by the system. In addition, the complexity of some AI models could lead to an inability to provide stakeholders with adequate explanations to understand and justify the decisions made by the system.

Example: Using and making public, e.g. on social media, content generated by AI systems without indicating that the content was produced by artificial intelligence systems.

- Health and Safety

AI systems, due to possible accuracy and robustness issues, can introduce significant risks to people's safety as well as their physical and mental health.

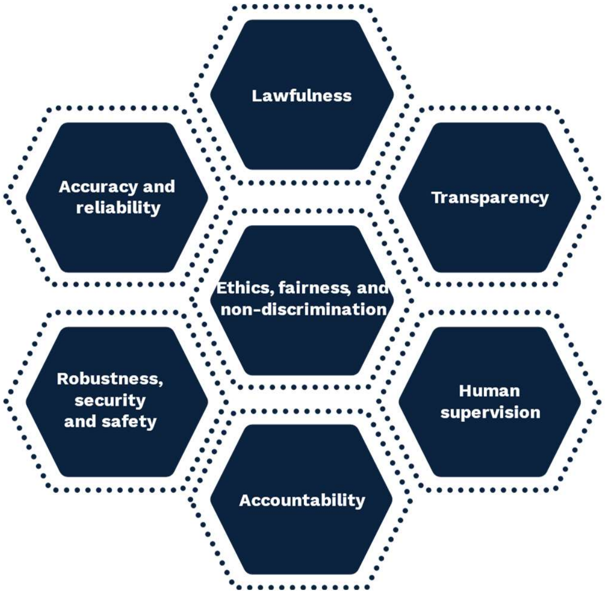
Example: If the machine vision system of a self-driving vehicle is unable to correctly detect a pedestrian crossing the road or another vehicle, the result could be an accident.

PRINCIPLES AND RULES FOR THE RESPONSIBLE USE OF AI

In dealing with the subject of artificial intelligence, ethics plays a crucial role in determining how this new technology should be developed, used and

integrated into Prysmian with respect for human values and fundamental rights so that the technology contributes positively to human wellbeing. To this end, Prysmian defines and adopts the Ethical Principles for Responsible AI, which derive from the Group's Code of Ethics and are based on a set of requirements identified in internationally relevant standards (e.g. Assessment List for Trustworthy AI (ALTAI) drawn up by the High-Level Expert Group on Artificial Intelligence established by the European Commission).

Figure 2: Principles for Responsible AI



- Lawfulness

Artificial intelligence systems must be used in compliance with applicable legislation, in particular about intellectual property (IP), privacy and personal data protection legislation, as well as any specific laws governing artificial intelligence.

- Accuracy and reliability

AI systems must produce precise, consistent, and dependable results, minimizing errors and biases to ensure high performance, and alignment with their intended purpose. Artificial intelligence is intended to improve human decisions, not to replace them.

- Transparency

The use of artificial intelligence systems must ensure that individuals are aware when they are engaged with AI technology and are provided with sufficient information to comprehend the main criteria, reasoning, and processes behind the system’s outputs or decisions.

- Ethics, fairness and non-discrimination

Artificial intelligence systems must be used in a responsible and ethical manner, respecting the dignity, freedom and diversity of individuals, and avoiding discriminatory impacts and unfair prejudices.

- Robustness, security and safety

Artificial intelligence systems must operate robustly, safely and securely throughout their lifetime, and potential risks must be constantly assessed and managed.

- Human supervision

Artificial intelligence systems must be used in such a way that human supervision of their outputs is always ensured, including to prevent consequences that may affect individuals, as well as erroneous, hallucinated or biased results.

- Accountability

All actors must be responsible for the use of AI systems and compliance with the above principles, according to their roles, the context and consistent with the state of the art.

RULES FOR THE RESPONSIBLE USE OF AI

When using AI, it is crucial to ensure that you do so responsibly and ethically. This implies that one should always consider whether it is appropriate to use AI for a specific use and, if one decides to use it, that the following guidelines are adhered to:

Prohibited behaviours

As provided for in the EU AI ACT, prohibited AI practices are prohibited, such as:

i. AI systems that use manipulative, subliminal or deceptive techniques;

ii. AI systems that exploit people's vulnerabilities;

iii. AI systems that assess and classify people on the basis of social behaviour and personal characteristics that result in prejudicial or unfavourable treatment in social contexts unrelated to the one in which the data were collected and/or unjustified or disproportionate to the behaviour;

iv. AI systems for assessing the risk of commission of criminal offences by natural persons;

v. AI systems for creating or extending facial recognition databases by untargeted scraping of facial images from the Internet or CCTV footage;

vi. AI systems for inferring a natural person's emotions in the workplace, except where the use of the AI system is intended to be deployed or placed on the market for security reasons;

vii. biometric categorisation systems that individually classify natural persons on the basis of their biometric data in order to draw inferences or conclusions about race, political opinions, trade union membership, religious or philosophical beliefs, sexual life or sexual orientation;

viii. the use of 'real time' remote biometric identification systems in publicly accessible areas for law enforcement purposes.

It is also mandatory to comply with all applicable regulatory obligations based on the level of risk identified with respect to the AI system and the role played by Prysmian in relation to each individual AI solution/system.

Furthermore, in compliance with the principle of accountability, it is forbidden to:

a) use company devices, credentials, e-mail addresses or telephone numbers to access publicly available AI tools (e.g. Chat GPT);

b) install unapproved AI-related Application Programming Interfaces, plug-ins, connectors or software;

c) implement or use, in any way, GenAI-generated codes on company systems;

d) use AI tools, in activities/projects involving third parties, without both parties having shared/approved their use and without specific contractual clauses on the matter.

- Mode and purpose of use

In accordance with the principle of accountability, it is necessary to ensure that the AI system is used exclusively for the purpose for which it was designed and in accordance with the instructions for use provided by the supplier.

Ensuring that the AI system is used in accordance with the instructions for use defined by the supplier is crucial both in terms of safety, as the system may not be optimized or safe for use other than its intended purpose, and in terms of regulatory compliance, as incorrect use may expose Prysmian to fines and penalties.

- Data export to unauthorized AI

It is prohibited to export, transfer, or share corporate data with third-party Artificial Intelligence tools that have not been explicitly approved by the B.O.D. of the Company and the Security & AI Committee. The use of certified corporate AI tools is the only permitted option for processing internal information, and any use of external AI must be pre-authorized.

- Personal data and business information

Unless specifically authorised, in compliance with the principles of lawfulness and minimization, no confidential, sensitive and reserved business information, including the personal data of employees and other business stakeholders, should be shared. In particular, as stated in the document “Data Classification Policy”:

- CONFIDENTIAL RESTRICTED – This is the highest classification level and identifies extremely confidential and business critical Information. The unauthorized disclosure outside of permitted distribution scope, loss, tampering or misuse represent a serious risk, in some cases irreversible, for the Group itself, its employees or third parties.
- CONFIDENTIAL – This level identifies highly sensitive Prysmian Group Information. An unauthorized access or release of this kind of Information poses a medium risk on the Group and its stakeholders.
- INTERNAL – This level identifies Information that does not belong to the previous levels and whose unauthorized access poses a low risk on the Group.
- PUBLIC – The unauthorized disclosure of the Information outside Prysmian Group does not pose any risk. Information of this kind is accessible to all users with no restrictions and/or publicly disclosed by the Group.

It is mandatory:

- Before uploading documents (including recording of meetings and transcription) to AI systems, verify whether they contain personal data or confidential commercial/corporate information.

- For any questions or clarifications regarding documentation and materials that may be uploaded to AI systems, including verification of the presence of personal data or commercial/corporate confidential information, please contact Prysmian’s Data Protection Officer (DPO).

- For any questions concerning what may constitute personal data and/or confidential commercial/corporate information, and generally concerning data protection issues, please contact the DPO.

When AI is implemented or hosted by a third party, any input will represent a "disclosure" of information to a third party. Not only will the third party have access to the input provided to it, but this input could be used to train the model and generate responses for other users. In fact, AI models can learn and reproduce the information in the training data. This can lead to the generation of outputs containing confidential information that, if shared or made public, could compromise confidentiality and security.

This means that anything that is entered into AI systems, particularly regarding personal data, must be treated as a disclosure of such information to a third party, subject to the requirements of applicable privacy and data protection laws. The same principle also applies to Prysmian's commercial and business information, including information falling under the category of trade secrets, which must be kept private and confidential, or third-party information for which Prysmian has confidentiality obligations.

In addition, it should be noted that the inclusion of personal data and business and company information in AI systems could entail significant risks for the individuals concerned and for Prysmian, in the event of a security incident or data breach.

Prysmian Group personnel, therefore, must always pay great attention to the type of data and information that is entered into AI tools/systems.

- Verification of AI output

In compliance with the principle of human oversight, AI output must not be used to fully automate a decision-making process, except for AI system outputs whose accuracy Prysmian has verified or confirmed.

In addition to this, in compliance with the GDPR, it is forbidden to automate, with the removal of the human operator, processes that use personal data and that may have a significant impact on individuals, regarding decisions that produce legal effects or significantly affect their personal or professional sphere.

It is mandatory to:

- Always verify the accuracy of the information received when using the Generative AI systems;

- Involve domain experts to verify the accuracy of the predictions or recommendations provided by the AI systems, with the exception of the previously mentioned cases;

- Before using the outputs, correct them if the verifications reveal errors or inaccuracies, or violation of privacy and/or inclusion of information/material protected by copyright or intellectual property of third parties or information/material not in line with the Prysmian Group's principles.

It is prohibited to:

- Use the outputs where the content is inappropriate, discriminatory (on the basis of race, religion, gender, origin, age, disability, marital status, political affiliation or sexual orientation) or otherwise harmful to the Prysmian Group and its stakeholders;

- Use Gen AI tools to create text, audio or visual content for fraudulent purposes or to misrepresent an individual's identity;

The output of artificial intelligence is based on statistical-probabilistic models and includes a built-in randomness factor. This implies that the output, although plausible, may be inaccurate or unreliable, manifesting itself in what is called a 'hallucination'. Furthermore, for generative artificial intelligence systems, even when using identical inputs, the output will not always be identical.

It is a known limitation that artificial intelligence systems may produce harmful, biased, incomplete, obsolete or false results, presenting these results with a seemingly confident tone, i.e. as if they were certain or fully reliable. In this context, users may place complete trust in incorrect, hallucinated or biased outputs, and make decisions and actions based on inaccurate or false information.

Therefore, it is crucial that one never uses something produced by artificial intelligence without first reviewing and verifying the accuracy of the output. Artificial intelligence is intended to enhance human decision-making, and make some company actions more efficient, never replace it.

- Intellectual Property

Unless specific authorisation has been provided, industrial property assets should not be provided as input to an AI system, nor should output that may infringe the copyright of others.

It is essential that you do not use or reproduce content subject to third-party copyright or intellectual property rights without an appropriate licence. Understanding and complying with applicable copyright laws and licence agreements is essential when employing pre-existing materials, such as images, text or music, as input for AI. Since AI solutions are trained using original works created by human beings, the output may infringe third-party rights if it is sufficiently like existing materials. Particularly risky examples include graphic works, such as logos.

- Ethical use and whistleblowing

The use of AI must comply with the ethical principles set out in this document and the Group's values set out in the Code of Ethics. If there is a suspicion of use that does not comply with these principles (e.g. gender discrimination in personnel selection), a report must be made through the DPO's reporting channel.

Furthermore, any suspected malfunctioning or interruption of the system's operation (e.g. loss of access to the system, disclosure of unnecessary personal data) must be immediately reported to privacy@prysmian.com and/or to the DPO, in line with the provisions of the procedures on security and privacy incidents, as described in the "Data Breach Incident Management".

It is essential to recognise that any unethical or improper conduct, which does not respect human dignity and freedom of individuals, and which is not in accordance with the principles and values promoted by Prysmian, is neither approved nor supported by Prysmian. Such conduct could jeopardise Prysmian's reputation and reliability, generating negative consequences for the Company, including potential financial impacts.

- Transparency on AI use

It is necessary to ensure maximum transparency, inside and outside the Prysmian Group, about how AI is used to support the business.

It is mandatory to:

- Inform your manager before you use an AI tool for the performance of a work activity
- Clearly attribute any output used for work purposes to the AI tool that generated it (e.g., through a footnote or other means visible to the reader, indicating that the content was generated through an AI tool and stating the name of that tool).

It is crucial never to present content produced by AI, either outside or inside Prysmian, without clearly stating the role of AI in the creation of such content. This includes, when necessary, an indication of the specific AI solution used.

Furthermore, if Generative AI is used to generate or manipulate visual, audio or video content, it must be made clear that such content has been artificially generated or modified.

7. OPERATING MODEL

AI GOVERNANCE AND COMPLIANCE FRAMEWORK

In line with this Policy, processes and procedures must be defined to support the effective management of artificial intelligence activities.

In particular:

- Identification and Inventory of AI Systems

The identification of AI systems refers to the process of recognizing a system as belonging to one of the various types of AI, taking into account distinct factors such as technical features, specific goals, and practical applications. This process requires an in-depth analysis of the system's operational capabilities, level of autonomy, learning methods, and underlying technologies, in order to understand how the system meets the needs it is designed for and the impact it may have in its context of use.

After identification, the AI system must be registered by the approved party, including all relevant system information. This process ensures transparency, oversight, and accountability, helping to monitor the safe and fair use of AI systems.

- Classification of AI Systems according to the EU AI ACT

The EU AI ACT introduces a risk-based classification for AI systems depending on their potential impact on fundamental rights, safety, and human health, aiming to ensure the safe, fair, and transparent development and use of AI. The classification process determines the risk category of the AI system, which defines the corresponding regulatory obligations.

- AI Risk Management

The AI risk management process identifies and assesses threats and risks associated with the development, implementation, and use of AI systems. Controls are defined and implemented to mitigate those risks. The process aims to ensure AI systems operate safely, ethically, and in compliance with regulations, minimizing negative impacts on individuals, organizations, and society as a whole.

- Regulatory Compliance

Depending on the AI system's risk classification, appropriate and proportional measures must be implemented to ensure full compliance with the obligations outlined in the EU AI ACT, as well as in other applicable regulations. These measures should be aligned with the nature and severity of the identified risk, to ensure that the development, deployment, and use of AI occurs safely, fairly, and transparently, while protecting fundamental rights, safety, and human health.

Protective actions, implemented through defined processes and procedures, must be applied proportionally to the value and risk level associated with AI systems, in accordance with the applicable regulatory framework.

To ensure safe and ethical AI system management, the established processes must ensure:

- Employees and stakeholders involved in the implementation and use of AI systems act in compliance with the company's responsible AI governance framework;
- Continuous improvement of AI systems management, with a focus on transparency, fairness, and risk mitigation.

Overall, Prysmian ensures that Artificial Intelligence systems are developed and managed in line with the above principles and in compliance with all applicable AI governance regulations and provisions.

SUSTAINABILITY IMPACT AND AI USE CONSIDERATIONS

The training of AI models requires the use of huge amounts of computational resources, as machine learning processes are highly complex and require intensive processing to analyse and handle large volumes of data. This significant use of computing power leads to high energy consumption, which not only affects the operating costs of IT infrastructures, but also has a considerable environmental impact. Indeed, the high energy requirements associated with these operations contribute to increased carbon emissions and pressure on natural resources, raising important sustainability issues in the development and implementation of AI technologies.

8. ORGANIZATIONAL MODEL

As part of AI systems governance, the primary business functions involved are identified, and their roles and responsibilities in AI management are defined.

MAIN AI MANAGEMENT ACTIVITIES

Compliance & DPO Office

- Identification of national and international AI regulations (e.g., EU AI ACT, GDPR, national implementing regulations);

- Responsible for ensuring the compliance of processes and reference documentation with current AI and data protection legislation;
- Supports the Office of CIOs in identifying the AI system risk classification, in accordance with EU AI ACT requirements;
- Impact assessment for regulatory compliance and fundamental rights, especially for high-risk systems;
- Supports departments in reporting serious incidents, particularly those related to high-risk systems.
- Provides specific training to all personnel involved in the use of AI systems, and prepares and updates training materials on AI systems, AI governance, and applicable legislation.
- Collaborates with other corporate functions (e.g., Legal, Risk Management, HR, IT, Security) to ensure integrated governance and alignment between data protection and AI compliance requirements.

Information & Cybersecurity

- Identification and assessment of cybersecurity risks related to AI implementation and use, ensuring appropriate management, especially for high-risk systems;
- Conducting independent tests and audits to verify compliance with security requirements, especially for high-risk systems (e.g., vulnerability analysis, attack simulations, data integrity checks);
- Defining an AI-specific incident response plan, particularly targeting vulnerabilities in high-risk systems;
- Promoting awareness of AI-related cybersecurity risks among stakeholders involved in AI projects;
- Oversee and coordinate AI-related incident response processes to ensure timely resolution and continuous improvement;
- Promote organizational AI literacy by developing training initiatives and resources that enhance understanding and responsible use of AI technologies.

Human Resources & Organization

- Oversight of AI’s potential for the workforce;
- Ensuring the use of AI aligns with corporate ethical values, promoting fair and non-discriminatory application;

- Promoting training initiatives on responsible AI use.

Purchasing Office

- Responsible for revising qualification and contracting processes with AI solution or service providers to include safeguards against legal risks, IP issues, and liability limitations;
- Responsible for notifying Legal and Corporate Affairs upon identifying procurement involving AI solutions.

Office of Corporate CIOs & Governance IT

- Responsible for verifying AI solutions and development processes adhere to Prysmian's Responsible AI Development Guidelines;
- Integrating AI risk management into the enterprise risk management system (e.g., identifying impacted compliance areas, establishing new controls);
- Responsible for setting up and monitoring data governance methodologies and tools, especially regarding the analysis of training and operational datasets for high-risk systems, identifying quality, representativeness, or bias issues;
- Responsible for storing, managing, and ensuring easy retrieval of all technical documentation related to AI systems;
- Responsible for implementing automatic logging systems that continuously and systematically record operations or situations posing potential AI system risks, especially for high-risk systems, ensuring accessibility for audit purposes;
- Responsible for maintaining the inventory of AI systems.

Intellectual Property

- Protection of Prysmian's intellectual property rights, with specific focus on safeguarding company data, content, and works that may be used to train artificial intelligence systems;
- Prevention of unauthorized use of third-party data, works, or copyrighted content in the development, training, or deployment of AI systems;
- Compliance with applicable laws and corporate policies regarding copyright, patents, trademarks, and utility models, in coordination with the relevant legal functions.

AI Governance Committee

Given the cross-functional nature of AI risks and opportunities, the Prysmian AI Governance Committee operates cooperatively and interdisciplinary across the above departments. It is tasked with:

- Evaluating AI proposals from a holistic perspective, including technical, operational, legal, and ethical dimensions. This includes technical feasibility, economic return, and ethical/reputational impacts. The committee collects input from various departments and provides risk management guidance, expressing an opinion on whether an AI initiative should proceed or identifying critical concerns to be addressed;
- Serving as a reference or escalation point for AI-related reports, complaints, or disputes, particularly those requiring impartial and multidisciplinary evaluation. It assesses associated risks and recommends corrective actions, fostering transparency and trust in AI systems;
- Promoting a responsible approach across the AI system lifecycle by defining overarching guidelines for development, testing, deployment, monitoring, and procurement. These ensure AI usage aligns with company values and the principles of transparency and sustainability.

9. CONSEQUENCES OF A POLICY VIOLATION

As a Prysmian Employee or Third Party, you are agreeing to uphold our commitment to ethical conduct and integrity and to abide by our Code of Ethics. Prysmian Employees who violate this commitment or do not comply with this Policy shall be subject to disciplinary procedures, including possible dismissal, and any other legal action required to protect the interest and reputation of Prysmian.

The Company reserves the right, at its sole discretion, to disclose information about violations of law by Prysmian employees to relevant regulatory agencies.

10. REPORTING A POLICY VIOLATION

As a Prysmian Employee, you are required to report any violation of this Policy to:

a) the **IF Helpline**, or

b) your Regional Compliance Team or the other designated subjects mentioned in this Policy.

11. AUDIT AND MONITORING

Using a risk-based approach, on a periodical basis the Group Compliance Function and the Internal Audit Department may perform, respectively, monitoring or audit activities aimed at verifying the correct enforcement of this Policy within the organization.

Consequences of violating the policy

The employees of the Prysmian Group agree to uphold our commitment to ethical conduct, integrity, and compliance with our Code of Ethics. Employees who violate this Policy will be subject to disciplinary procedures, including potential termination, as well as any other legal actions necessary to protect the interests and reputation of the Prysmian Group.

Business partners and third parties acting on behalf of the Company who violate this Policy will be subject to financial and legal consequences, where applicable, including contract termination and prohibition from engaging in business relations with the Prysmian Group.

12. REVIEW

Artificial Intelligence is a field of continuous and rapid evolution, marked by significant advancements and constant innovations. In this context, Prysmian is committed to periodically reviewing this policy to ensure it remains relevant and up to date with the latest trends and developments in the AI sector. It is essential to regularly consult this policy, as it contains valuable guidance and crucial updates to ensure the responsible and compliant use of AI technologies within the organization. This proactive approach will enable Prysmian to address emerging challenges and capitalize on the opportunities offered by AI to the fullest extent.

13. RELATED DOCUMENTS

The following Documents are related to this Policy and must be consulted by all Prysmian Employees for further guidance. Part of such documents are available on the Prysmian Ethics & Integrity Homepage of our **Company's Intranet** and are also publicly available within the correspondent section of our **Corporate website.**

a) Code of Ethics;
b) Helpline Policy.