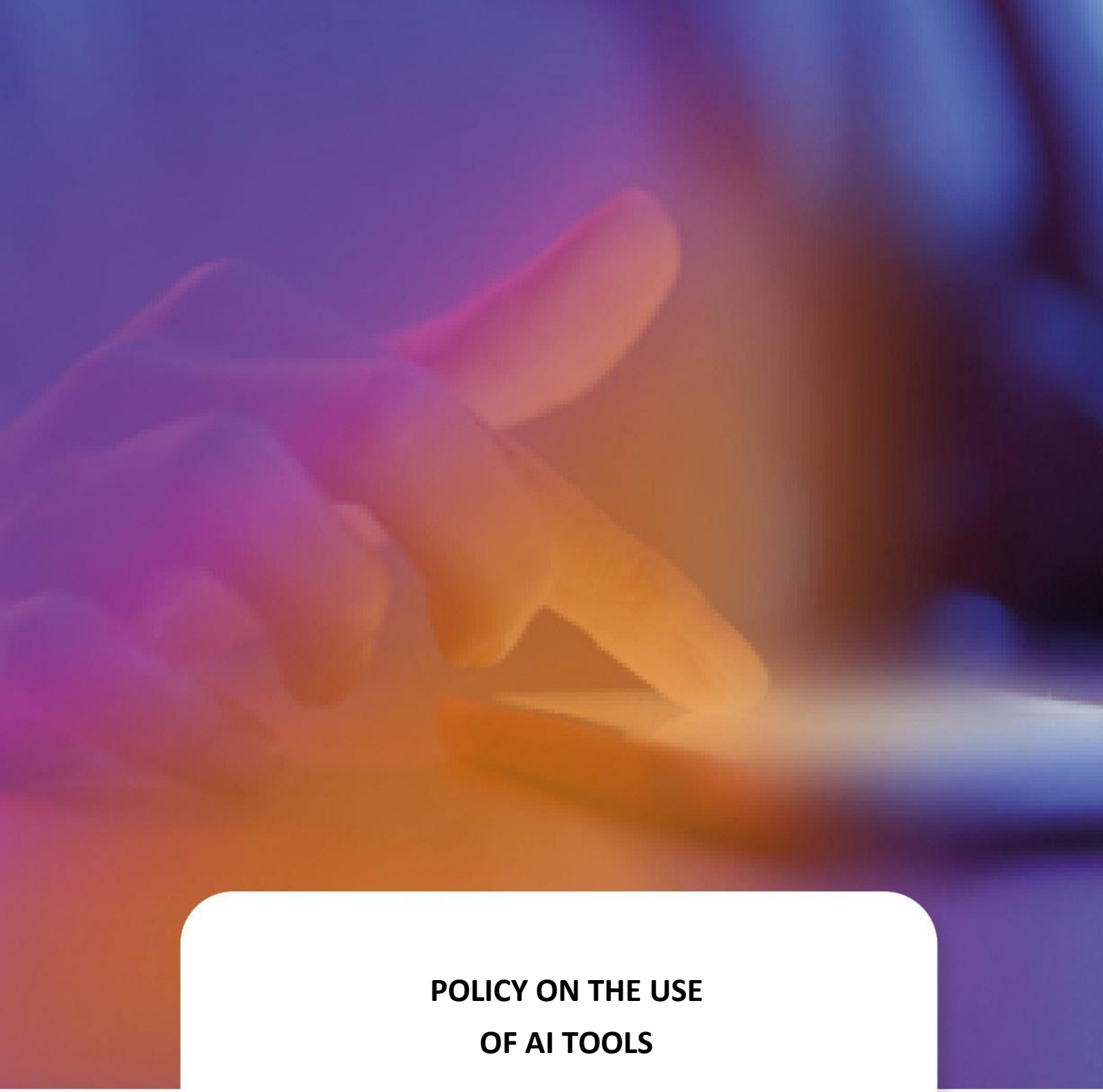


POLICY ON THE USE OF AI TOOLS

Version 1.0 of 07/10/2026

INDEX

1.1. _____ **1**

1. Introduction _____ ***3***

1.2. Context of reference _____ **3**

1.3. Regulatory references _____ **3**

1.3.1. Mandatory legislation _____ 3

1.3.2. Internal regulations _____ 3

1.4. Objectives _____ **5**

1.5. Definitions and terminology _____ **5**

2. Scope _____ ***8***

3. General principles of artificial intelligence _____ ***9***

3.1. Robustness, accuracy, and safety of AI systems _____ **9**

3.2. Protection of personal data and intellectual property _____ **9**

3.3. Human Oversight _____ **10**

3.3.1. Human in the Loop _____ 10

3.4. Transparency and explainability _____ **10**

3.5. Fairness and non-discrimination _____ **11**

4. Process for the development and responsible use of AI Systems _____ ***12***

4.1. Documentation, traceability and lifecycle management of AI systems _____ **12**

5. Reporting _____ ***12***

6. AI training _____ ***13***

7. AI Policy Review _____ ***13***

1. Introduction

1.1. Context of reference

Artificial intelligence (hereinafter referred to as "AI") is an enabler for innovation, operational efficiency and the quality of the services offered by the TAS Group (hereinafter also referred to as "TAS"). The evolution of generative, predictive and analytical technologies opens up new opportunities in software development support, document management, process optimization and user experience improvement.
At the same time, the adoption of these technologies introduces significant risks in terms of information security, intellectual property, data protection, accuracy of results and reliability of systems. This AI Policy (hereinafter the "Policy") defines the principles that guide the use, development and responsible integration of AI in the TAS Group. It provides a unified reference framework, consistent with European and national legislation on the subject, ensuring a prudent, ethical approach oriented towards the protection of information assets and corporate reputation. The aim is to promote the use of AI that amplifies people's skills, safeguards data confidentiality, guarantees transparent behaviour and maintains high standards of quality and security throughout the life cycle of the systems.

1.2. Regulatory references

1.2.1. Mandatory legislation

- Regulation (EU) 2024/1689 (AI Act);
- Regulation (EU) 2016/679 (GDPR);
- Directive (EU) 2022/2555 (NIS2);
- Regulation (EU) 2022/2554 (DORA);
- Law 300/1970 (Workers' Statute, in particular Art. 4);
- L. 633/1941 and Directive (EU) 2019/790 (Copyright);
- Legislative Decree 231/2001 (Regulation of the administrative liability of legal persons);
- Technical and industry regulations on information security, intellectual property protection and data classification;

1.2.2. Internal regulations

- Company regulations and disciplinary code
- Company Code of Ethics
- Organisational and Management Model pursuant to Legislative Decree 231/01
- SQPRC052-Adoption and management of Artificial Intelligence systems
- SQPRC001- Management of quality system documented information
- SQPRC002-Training Management
- SQPRC012- Software solutions design and development
- SQPRC013- Services planning delivery and monitoring
- SQPRC019- Test preparation and execution

- SQPRC022- IT solutions assistance and maintenance
- SQPRC031-Security incident management
- SQPRC034- Privacy-Regulatory compliance
- SQPRC035-BIA and risk assessment
- SQPRC046- Planning and management security scans
- SQPRC047-Vulnerability identification and management
- SQPRC044- Whistleblowing Other companies
- SQPRC045- Whistleblowing TAS

1.3.Objectives

The Policy pursues the following objectives:

- promote the safe, ethical and responsible use of AI to foster the dissemination of competence and awareness among staff and to prevent - as far as possible - errors, biases or unexpected behaviour;
- protect the personal data, intellectual property and information assets of the TAS Group;
- ensure that AI supports human skills and does not replace them;
- ensure the full compliance of business processes with applicable European and national regulations, adopting a risk-based approach in line with the AI Act, the GDPR and the security requirements of networks and information systems (DORA and NIS2);
- ensure the transparency, traceability and explainability of AI-based solutions, strengthening the trust of customers and stakeholders in the products and services provided by the Group;
- direct technological innovation towards the continuous improvement of operational efficiency and the quality of the artifacts produced (e.g. software, documentation), maintaining at every stage the mandatory obligation of human control over decision-making processes;
- promote the development and adoption of AI systems that comply with sustainability criteria (ESG) and the values of the company's Code of Ethics, repudiating any form of algorithmic discrimination or violation of fundamental rights.

1.4. Definitions and terminology

Personal Data	Any information relating to an identified or identifiable natural person. An identifiable person is one who can be recognised, directly or indirectly, by means of such things as a name, an identification number, location data, an online identifier or other factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person.
Recipient	Subject who suffers or may suffer the effects generated by the AI System, even in the absence of direct interaction with it. This subject may coincide, in certain circumstances, with the User.
Serious/Disastrous Incident	An event that has a serious/disastrous impact (according to the company classification referred to in the SQPRC035-BIA and risk assessment procedure), on the safety of individuals, on the protection of personal data, on the reliability of business processes or on respect for

	fundamental rights. Under the AI Act, an incident is considered serious when it causes, or is reasonably likely to cause, significant damage to natural persons, significant loss or compromise of data, or harmful effects on critical assets, activities or proceedings.
AI model	The algorithmic component trained on data that allows an AI system to produce a certain type of output.
Prohibited AI practices	Categories of use of artificial intelligence expressly prohibited by the AI Act as they are considered contrary to the fundamental rights, safety or dignity of the person. Prohibited practices include, but are not limited to, systems designed to manipulate human behavior through subliminal techniques or by exploiting specific vulnerabilities; social scoring systems applied to natural persons; the use of technologies that allow real-time biometric recognition in publicly accessible spaces outside of permitted cases; as well as any application that poses an excessive risk to public safety or the integrity of democratic processes.
AI risk	Potential adverse effects from the use of an AI System, including risks to data security, output quality, intellectual property protection, or impact on people and processes.
Artificial Intelligence (AI) System	A system based on algorithmic or statistical models capable of generating outputs such as forecasts, recommendations, content or decisions that affect physical or virtual environments.
Generative AI system	An AI system designed to generate new and original content — such as text, code, images, or analytics — based on models trained on large amounts of data.
High-Risk AI / Limited Risk AI	Risk categories under the AI Act, which classify AI systems according to their potential impact on rights, safety or critical processes. Different levels of risk correspond to proportionate safeguards.

Human Oversight	The ability for people to monitor, understand and intervene on the results generated by an AI system in order to ensure its safe and effective use.
Human in the Loop (HITL)	Modes of use of AI in which human input is an integral part of the process, through the verification, correction or validation of the outputs generated by the model before their operational use.
Algorithmic bias	Unintentional deviation in data or patterns that can result in biased or discriminatory results.
Technical documentation	Minimum set of information necessary to describe the operation, characteristics, methods of use and outputs of an AI System, useful for ensuring transparency, control and correct maintenance.
AI System Lifecycle	The set of phases that make up the existence of an AI system, from the preliminary assessment of the use case to the development, validation, use, monitoring and updating.
Fallback (or deactivation mechanism)	Ability to suspend or replace the use of the AI System when the output is unreliable, inadequate or risky, ensuring business continuity through alternative procedures.

2. Scope

The following Policy applies:

- to all TAS Group companies that use or implement AI systems;
- to all employees, collaborators, consultants and suppliers authorized to access AI tools or models owned by TAS;
- any use, direct or indirect, of platforms, services, models or tools that incorporate generative or non-generative AI functions.

It only regulates the Principles and not the operating methods, which are regulated in the specific company procedures.

The TAS Group recognises that AI systems present different levels of risk, in accordance with the European regulatory framework[1]. The use of AI solutions therefore involves the adoption of measures proportionate to the level of risk, distinguishing between low, moderate or high risk systems.

[1] As defined in Regulation (EU) 2024/1689 (AI Act).

3. General principles of artificial intelligence

The adoption of artificial intelligence within the TAS Group is guided by a set of fundamental principles that guide every activity related to its development, use and integration into business processes. These principles represent a stable and transversal orientation, aimed at ensuring that the use of AI takes place in a safe, ethical, transparent manner that is compatible with the quality standards that distinguish the Group's operations.

3.1. Robustness, accuracy, and safety of AI systems

The security of information and systems is an essential requirement for any artificial intelligence application. AI must be designed and used in such a way as to ensure adequate levels of safety *and* cybersecurity, preventing risks that may compromise data integrity, business continuity or the quality of business processes.

Robustness and accuracy are fundamental elements of this principle. Robustness expresses the ability of the model to maintain reliable and consistent behavior even when it is exposed to variations, noise, unexpected inputs or conditions that do not perfectly adhere to the training context. Accuracy concerns the correctness, relevance and consistency of the results generated with respect to the purpose pursued.

All staff must be aware that AI models, while advanced, can produce incomplete, incorrect or biased outputs.

It is therefore necessary to adopt a critical and prudent approach, verifying the validity of the results and applying, where appropriate, additional controls or manual corrections. The aim is to ensure that the use of AI does not introduce uncontrolled risks and that the systems used contribute in a reliable, secure and transparent way to the quality of business activities.

3.2. Protection of personal data and intellectual property

The TAS Group's information assets – which include personal data, source codes, technical documentation, application logics and customer data – represent a strategic asset. Every interaction with AI systems must comply with the requirements of the GDPR, internal data classification policies and intellectual property protection rules.

It is forbidden to share confidential, confidential or sensitive information with AI platforms that do not offer adequate guarantees in terms of data protection, storage and processing. The principle of minimization requires limiting the exchange of information to the minimum necessary, using the company tools made available for work activities.

TAS, in the choice of AI tools, makes the transfer of data to providers subject to non-EU jurisdictions (in particular the USA) subject to strict controls. In addition to verifying adherence to adequacy decisions or signing SCCs, the Company assesses the risk of interference by foreign government authorities governed by surveillance regulations. Where necessary, the Company requires the adoption of additional technical measures (e.g. encryption) to protect data subjects.

3.3. Human Oversight

The TAS Group places a central role on human supervision in the process of using AI. Each output must be examined, validated and contextualized, so as to ensure that the results generated are consistent, accurate and fit for purpose. Human supervision prevents misinterpretations, reduces the risk of errors and ensures that AI remains a supporting tool and not a substitute for human judgment.

3.3.1. Human in the Loop

In line with the internal procedures and principles promoted by the TAS Group, the concept of Human in the Loop represents a concrete declination of human control over artificial intelligence. It envisages that human intervention is not only possible or residual, but an integral part of the process of using AI, with an active and decisive role in evaluating, confirming or correcting the results generated.

The Human in the Loop approach implies that each AI output is subjected to a qualitative and functional verification before being definitively used in business processes. This means that people retain control over the decisions that AI can influence, ensuring that the analyses carried out by the models or the content generated are consistent, accurate and fully responsive to organizational expectations. This principle guarantees full compliance with Art. 22 of the GDPR, ensuring data subjects' right not to be subject to a decision based solely on automated processing that produces legal effects.

This principle is particularly relevant in contexts where AI supports technical or documentary tasks, such as code development, text editing, content classification, or processing information that has a potential operational impact. In cases where AI generates portions of code or textual rework, competent personnel are called upon to carefully examine these results, integrate them with their own professional judgment and validate them before they are incorporated into business systems, processes or documentation.

As part of the Human in the Loop principle, staff retain the ability to intervene, correct or replace the result produced by AI if it is inadequate, incomplete or potentially harmful. This includes the ability to suspend the use of the tool or to resort to alternative ways of carrying out the activity, implementing forms of "fallback" that ensure business continuity and process quality even in the presence of unexpected model behavior.

3.4.Transparency and explainability

The use of AI must be transparent: employees must be aware of the purposes, general logics and limitations of the tools used. When necessary, solutions must be adopted that allow them to adequately understand the reasons that led to a certain result, so as to allow a critical and informed evaluation.

Explainability is an essential element of such transparency. It implies the ability for the user to understand in clear and understandable terms how the main logics of the model work and the factors that influenced the output generated. Proper explainability builds trust, allows for the identification of any errors or biases, and allows staff to exercise informed control over the results produced by the AI.

Where applicable, TAS is also committed to ensuring that customers are also informed in a clear and understandable way of the use of Artificial Intelligence systems in the services and products offered, in line with the principles of transparency, fairness and current regulations.

3.5. Fairness and non-discrimination

Artificial intelligence must be used in a way that avoids unjustified processing or discriminatory effects, whether intentional or unintended. When the use case requires it, attention should be paid to the quality, representativeness and balance of the data used, so as to prevent biases that may be reflected in the results generated.

The TAS Group promotes an approach based on fairness and impartiality, requiring that any bias or anomalies detected be addressed promptly, adopting appropriate corrective measures to ensure the fairness of the processes supported by AI.

4. Process for the development and responsible use of AI Systems

The use of artificial intelligence tools must take place with a sense of responsibility, technical awareness and full adherence to the principles set out in this Policy. In particular, TAS promotes an approach that favors the use of business solutions or platforms that offer adequate guarantees of data protection and protection of information assets. The use of free or publicly accessible tools is allowed only when it is certain that the information processed does not contain confidential or proprietary elements, nor personal data or portions of proprietary code.

Any interaction with AI systems must be conducted in a way that avoids the inadvertent disclosure of sensitive information. This implies that the selection of tools cannot be based solely on intuitiveness or ease of use, but must prioritise the risks related to data retention, how the provider processes it and possible contractual implications.

In the context of software development, the use of AI can be a valuable aid in speeding up activities, identifying errors or generating alternative solutions; however, the code produced cannot be accepted uncritically or introduced into projects without a thorough technical review. Developers are called upon to verify the logical correctness of the code, its compliance with internal standards and the compatibility of the licenses associated with the tools used. The use of AI must never lead to a loss of control over software artifacts or to the compromise of the quality of the final product.

Similarly, with regard to document management, it is essential to carefully assess which content is suitable for processing using AI tools. Generic texts or texts without confidential information can be treated with more flexibility, while classified documentation requires a higher level of protection and cannot be shared with tools that do not ensure adequate levels of security. Staff are therefore required to carry out a prior assessment of the content before using it within AI tools.

TAS adopts a risk-based process for developing, integrating, and using AI systems.

The methods of preliminary assessment, verification of compliance, approval and monitoring are governed by the procedure SQPRC052-Adoption and management of Artificial Intelligence systems and the related operating instructions.

4.1. Documentation, traceability and lifecycle management of AI systems

TAS recognizes the importance of traceability and documentation in the use of AI systems, promoting responsible management of the life cycle of models to ensure the reconstructability of decision-making processes, as governed by company procedures.

5. Reporting

Mature and responsible use of artificial intelligence implies the ability to recognize, intercept and promptly manage anomalies or vulnerabilities.

Personnel are required to report without delay, as defined by the SQPRC052-Adoption and management of Artificial Intelligence systems procedure, any unexpected behaviour, bias or risk to the security and confidentiality of data. If the report concerns situations involving violations of the company's Code of Ethics or unlawful conduct or potential offences pursuant to Legislative Decree 231/01 committed using AI tools, personnel must use the whistleblowing channels adopted by the company and defined by the procedures SQPRC044- Whistleblowing Other companies and SQPRC045-

Whistleblowing TAS, designed to guarantee the necessary confidentiality protections provided for by current legislation.

Failure to comply with these principles and failure to report incidents according to the company channels set up constitute violations punishable under the Company Regulations and Disciplinary Code.

6. AI training

The correct adoption of AI requires that personnel have an adequate level of knowledge of the risks and opportunities associated with this technology. TAS therefore adopts, in compliance with Article 4 of EU Regulation 2024/1689 (AI Act), training initiatives aimed at fostering the competent and informed use of AI tools, providing guidance on the principles to be respected, the correct methods of interaction and the tools approved for business use.

TAS, as defined by the procedure SQPRC052-Adoption and management of Artificial Intelligence systems, promotes training initiatives aimed to:

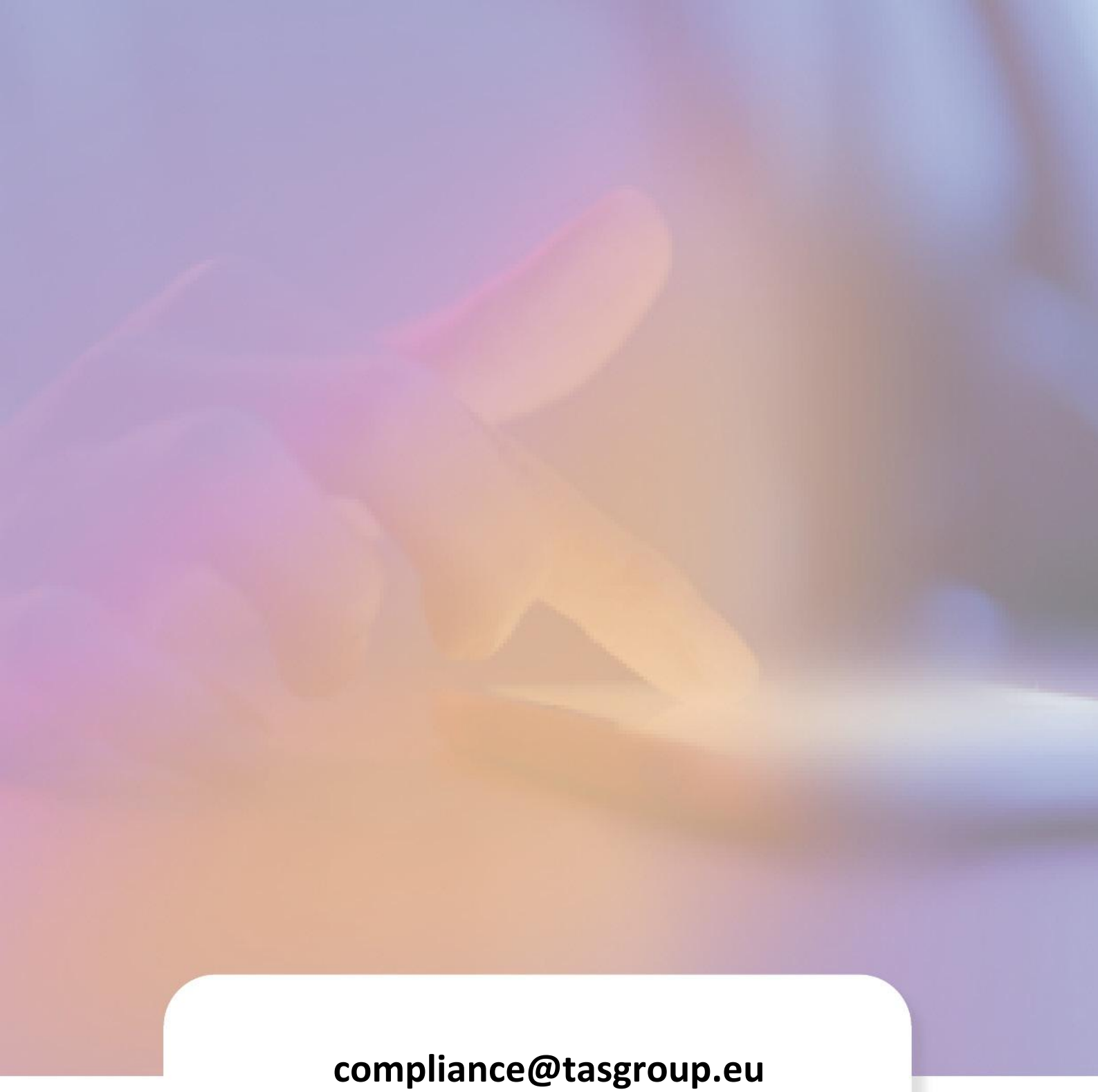
- raise awareness of the risks and opportunities of AI;
- encourage a competent and critical use of the tools;
- provide information on approved tools and correct methods of use;
- disseminate knowledge of internal procedures and applicable regulations.

Training is calibrated according to roles, skills and use cases, and is planned and managed by the Training Office according to the SQPRC002-Training Management procedure.

7. AI Policy Review

This Policy is subject to at least annual review and extraordinary revision if the need arises, both as a result of updates to current regulations and for events that change the risk profile (e.g. but not limited to the structural introduction of new AI tools, geopolitical events that may lead to a re-evaluation of the tools adopted, events/reports deriving from the operational use of AI in business processes, etc.).

Any changes are managed in accordance with the SQPRC001- Management of quality system documented information procedure of the management system.



compliance@tasgroup.eu