



POLICY ON THE USE AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE SYSTEMS

Welcome to TESISQUARE®

CONNECTING PEOPLE, TECHNOLOGY,
AND PROCESSES IN A COLLABORATION SQUARE

Review and approval

ACTION	FUNCTION	NAME	DATE
Approved	President	Giuseppe Pacotto	02/04/2024
Verified	Legal Manager	Alessandro Cassinelli	02/04/2024
Written by	Legal & Privacy	Alice Vanni	02/04/2024
Update	Legal & Privacy	Claudia Amelia Urbano	23/09/2026

Update

VERSION	DATE	NOTES
1.0	02/04/2024	Document creation
2.0	23/09/2026	Document update

FOREWORD

The purpose of this Policy is to incorporate, on an ongoing basis and in accordance with the characteristics of the business model, the guidelines regarding ethical considerations established by the European Union and the Organization for Security and Cooperation in Europe (OSCE), with regard to the governance of the artificial intelligence models used by TESISQUARE (hereinafter “Artificial Intelligence” or “AI”).

In particular, at the time of writing, the relevant regulations and guidelines are as follows:

1. OECD, Council Recommendation on Artificial Intelligence of 22 May 2019 (OECD/Legal/0449, Recommendation of the Council on Artificial Intelligence);
2. Regulation (EU) 2024/1689 – the AI ACT, which came into force on 1 August 2024;
3. Regulation (EU) 2026/1744 (Digital Omnibus on AI), which entered into force on 27 July 2026.

TESISQUARE recognizes the importance of addressing the challenges associated with the use of AI and of taking its ethical implications into account. In this regard, TESISQUARE continuously monitors regulatory developments, including at the level of regulations and guidelines, to ensure the accurate and timely implementation and adaptation of its internal policies, where deemed appropriate, progressively aligning its procedures with key regulatory deadlines (e.g. general application in August 2026, the entry into force of absolute bans in December 2026 and obligations for high-risk systems in December 2027).

The following chapters describe the principles that guide TESISQUARE's approach to this issue, clearly distinguishing the responsibilities associated with the two operational roles held by the Company (User/Deployer and Supplier/Provider)

1. Policy

TESISQUARE recognizes the transformative potential of Artificial Intelligence, but is aware of the risks that may arise from its use and is therefore committed to using it in an ethical, responsible and secure manner to improve the efficiency, innovation and quality of the products and services offered to its customers, and in all cases in accordance with this Policy.

TESISQUARE has identified two key areas in the use of AI:

1. **Efficiency of internal processes:** TESISQUARE aims to support decision-making and production processes through the use of AI. For example, software utilizing AI enables data analysis and extraction to be carried out more quickly and accurately than manual analysis and extraction; it can assist TESISQUARE staff with repetitive and standardized tasks; and it can also help product development teams with writing source code (operating exclusively within structured and controlled corporate environments, such as Cursor Teams or Microsoft Copilot Enterprise).
2. **AI in TESISQUARE's products and services (as a supplier/provider):** TESISQUARE aims to develop and market products (software or algorithms, such as its proprietary solutions

AgentDoc, Cogito and Synapse) that harness the potential of Artificial Intelligence, with a view to improving its clients' business processes and promoting innovative digital solutions. In developing these products and services, TESISQUARE uses exclusively Artificial Intelligence models provided by qualified technology partners, whose tools are licensed and are carefully selected and verified. TESISQUARE ensures that these models comply with current legislation on the protection of personal data (GDPR) and the European Artificial Intelligence Regulation (AI Act), in accordance with the principles of security, transparency, reliability and accountability.

The AI applications used in TESISQUARE and developed by TESISQUARE for its clients will be subject to ongoing assessment to monitor their performance, fairness and compliance with the principles set out in this Policy. Any issues identified will be addressed and rectified promptly.

TESISQUARE promotes and ensures AI literacy amongst its staff, as defined by the Omnibus Regulation (EU 2026/1744) as an obligation of means aimed at raising adequate awareness of the risks, limitations and correct use of technologies (Article 4 of the AI Act).

2. Recipients

This Policy is addressed to all employees of TESISQUARE and to the associated companies and subsidiaries of TESISQUARE S.p.A., as well as to the various stakeholders of TESISQUARE who will read and accept its contents. The provisions contained in these Regulations are binding and apply without distinction to anyone working, in any capacity and under any type of contract, within the company's scope of operations or in the Company's interests (including managers, semi-subordinate employees, temporary workers, interns, external consultants and service providers).

3. General guiding principles

Whether using AI to improve and make its internal processes more efficient, or in the development and commercialization of AI, TESISQUARE adheres to the following guidelines.

Compliance with the law. TESISQUARE **is committed to complying with all applicable laws** and regulations concerning AI, ensuring full compliance and adaptation to any regulatory updates. TESISQUARE operates in full compliance with Regulation (EU) 2024/1689 (AI Act) and the amendments introduced by Regulation (EU) 2026/1744 (Digital Omnibus). The regulatory framework adopts a risk-based approach and imposes obligations on suppliers and developers of AI systems based on different risk levels: **unacceptable risk, high risk, limited risk and minimal or no risk**. TESISQUARE is committed to complying with these provisions. Consequently, TESISQUARE does not use or develop, by way of example, AI systems that employ subliminal techniques which operate without a person being aware of them; AI systems that target the vulnerabilities of a specific group of people, due to age or physical or mental disability, with the aim of materially distorting the behavior of a person belonging to that group; AI systems that enable the assessment or classification of the reliability of individuals over a given period of time on the basis of their social behavior or known or predicted personal or personality characteristics; real-time remote biometric identification systems in publicly accessible spaces; biometric categorization systems that use sensitive characteristics such as gender, race, ethnicity, nationality, religion or political orientation,

as well as systems for generating or manipulating non-consensual intimate or sexually explicit content (deepfakes). With regard to the use and marketing of other systems classified as high, limited or zero risk, TESISQUARE undertakes to comply with the obligations set out in the AI ACT and this Policy.

'The human is in control' (Human-in-the-Loop: HITL) and the principle of responsibility. AI is viewed by TESISQUARE as a simple tool. At any time, people can decide when and how to use the results provided by the tool. This is what happens, for example, when a machine assists humans with classification tasks. AI must be used as a tool to support human decision-making, not as a substitute. Important decisions must always be made by human beings. Closely linked to this principle is the principle of accountability. **AI outputs can support human decision-making, but they cannot replace human decisions.** In accordance with the principle of human oversight, any output or suggestion produced by an AI must be regarded as a mere working proposal. This means that AI outputs must always be subject to supervision by staff responsible for using AI applications. For example, the use of generative AI systems to write source code does not exempt the developer from verifying the correctness, integrity and compatibility of the code produced; similarly, the generation of images or posts intended for a social network via AI systems does not exempt the user from verifying that the image or post does not infringe the intellectual property rights of third parties. For proprietary solutions, human validation must take place via dedicated interfaces, such as the Validator GUI for AgentDoc and the feedback mechanisms (Thumbs up/down) for Cogito and Synapse. AI systems are often 'black boxes' and their outputs should be used with great caution.

4. Specific guiding principles relating to the use of AI

TESISQUARE believes that AI can help to improve the quality of certain internal processes and make them more efficient, in accordance with the following principles.

Confidentiality and the protection of TESISQUARE's know-how and intellectual property, and the prevention of 'Shadow AI'. Company data and information, and in particular the source code for TESISQUARE software, are a key asset for TESISQUARE. **Users are prohibited from feeding TESISQUARE's confidential business information into language models that are accessible to the public** (such as the free versions of ChatGPT, Gemini or Claude). In order to prevent the risk of data leaks and cyber vulnerabilities, authorized staff must carry out their activities exclusively within the secure environments contracted by Tesisquare at Enterprise level. When interacting with authorized AI tools, Recipients are required to apply safe prompting rules, refraining from including personally identifiable data, confidential information or critical portions of proprietary code in their prompts.

GDPR, personal data protection and employment law safeguards. Users are prohibited from feeding personal data into AI systems, particularly those accessible to the public. Such processing of personal data is not, in fact, recorded in the company's privacy notices or in the Data Processing Register and must therefore be regarded as unlawful. For example, **it is prohibited to use AI systems to extract data relating to TESISQUARE employees or customers, or to screen CVs using AI systems.** To this end, within the context of human resources management, Tesisquare strictly prohibits the adoption of individual measures that significantly affect the working lives of employees or candidates based solely on automated processing. Any corporate decision taken without effective and critical human intervention is to be considered legally null and void. Any

form of psychological, emotional or behavioral profiling of workers is also prohibited, in order to prevent internal systems from being reclassified as High-Risk systems (Annex III of the AI Act). Any exception to this prohibition must be approved by TESISQUARE, subject to verification by the Legal Department, so that the appropriate impact assessments can be carried out.

Transparency. The use of artificial intelligence systems to produce a specific output (a slide, an analysis, a report, etc.) must always be disclosed to the person you are communicating with. This does not mean that every single prompt given to an AI system must be disclosed; for example, it is possible to write a report yourself whilst occasionally consulting an AI system on certain sections where you have doubts. However, if the report has been generated entirely by an AI system, you are obliged to state this, keeping in mind at all times that ultimate responsibility for its content always lies with the person who queried the AI system to produce the report.

Caution. Due to the opacity of the internal processes of neural networks and the inaccessibility of all the data processed simultaneously by deep learning-based AI systems, AI systems are sometimes referred to as 'black boxes'. Although the AI system works because it produces outputs that are consistent with the prompts, we do not know exactly how it achieves these results or which data most influence its decisions, unlike traditional computer programmers, where all the code has been compiled in a controlled manner and with extensive human intervention. This situation requires AI users to **exercise greater caution** whenever they use AI systems to generate content, documents, analyses or reports, as the output could infringe the rights of third parties (for example, the generation of source code owned by third parties, or the generation of an image of a person to be used in a marketing campaign that corresponds to a real-life individual). If in doubt, please contact the Legal Department.

5. Specific guiding principles relating to the development and marketing of AI systems to TESISQUARE's customers

TESISQUARE is committed to developing and supplying its clients with AI systems that comply with the law (and in particular with the provisions of the AI Act) and with the guidelines set out from time to time by national and international bodies involved in AI matters, whilst adhering to the following principles and in accordance with the philosophy of 'compliance by design', by incorporating technical safeguards, transparency mechanisms and human oversight systems directly into the software architecture (e.g. through the AgentDoc, Cogito and Synapse solutions).

Responsible use of customer data. TESISQUARE is responsible for safeguarding a large volume of its customers' data. The use of this data for advanced analysis using AI systems is carried out in a **transparent and explicit manner, in compliance with confidentiality obligations and the requirements imposed by the GDPR and other applicable laws**. Therefore, all computing and storage infrastructure is located within the European Union (EU Data Residency) and customer data is never used to train public models. TESISQUARE uses customer data responsibly, addressing any legal and ethical issues that arise on a case-by-case basis.

Transparency. AI systems **are designed and developed in such a way as to ensure that their operation is sufficiently transparent** to enable users to interpret the system's output and use it appropriately. TESISQUARE guarantees that AI systems are designed and developed in such a way that individuals are informed that they are interacting with an AI system (in accordance with the

transparency requirement under Article 50 of the AI Act, via notices integrated into the interface that cannot be disabled), unless this is already evident from the circumstances and context of use.

Traceability and explainability. TESISQUARE designs and distributes AI systems capable of automatically recording events (logs) whilst in operation, ensuring they are securely stored for a minimum period of six months. It also provides appropriate technical documentation describing their operation and training procedures.

Safety. TESISQUARE designs and distributes AI systems in such a way as to ensure, in light of their intended purpose, an appropriate level of accuracy, resilience and cybersecurity, and to operate in a manner consistent with these aspects throughout their entire lifecycle, implementing effective solutions against AI-specific threats such as prompt injection.

Supply chain liability and contracts with third parties (Article 25). When developing its solutions, TESISQUARE enters into written supply chain agreements with upstream suppliers of general-purpose models (GPAI), ensuring that it receives the necessary technical information and mitigating systemic risks. At the same time, in contracts entered into with external parties (consultants, suppliers) who interact with the company's systems, TESISQUARE requires the mandatory inclusion of clauses in accordance with Article 25 of the AI Act.

6. Periodic review

This Regulation is subject to an annual review and update, carried out by the Legal Department in close coordination with the CISO, the AI Competence Centre and the DPO, to ensure that it remains aligned with evolving technological, ethical and regulatory developments in the field of AI.

7. Consequences of the inspections

Any breach of the requirements and prohibitions set out in these Regulations constitutes a disciplinary offence and a breach of contractual obligations. Such conduct will be sanctioned in accordance with the procedures laid down in the applicable National Collective Labour Agreement (CCNL). In the event of a breach of the principles of this Policy, TESISQUARE shall be entitled to take action against the person concerned by raising a claim of breach of contract in the manner provided for by law and by the contract itself. Where the breaches committed constitute criminal offences or conduct likely to give rise to the Company's administrative liability, the relevant proceedings will be coordinated with the disciplinary system of the Organization and Management Model pursuant to Legislative Decree 231/2001 (MOG 231).