POLICY SULL'UTILIZZO E SULLO SVILUPPO DI SISTEMI DI INTELLIGENZA ARTIFICIALE

Welcome to TESISQUARE®

CONNECTING PEOPLE, TECHNOLOGY,
AND PROCESSES IN A COLLABORATION SQUARE

TESISQUARE SpA Registered office: Via Mendicità Istruita, 24 – 12042 Bra (CN) - Headquarters: Via Savigliano, 48 - 12062 Roreto di Cherasco (CN)
Phone +39 0172 476301 - Fax +39 0172 476399 - www.tesisquare.com - info@tesisquare.com
Tax Code and VAT no. 02448510046 – Cuneo Chamber of Commerce - Economic and Administrative Register no. 177331
Share Capital € 750,000 fully vested

Revisione e approvazione

AZIONE	FUNZIONE	NOME	DATA
Approvato	CEO	Giuseppe Pacotto	02/04/2024
Verificato	Legal Manager	Alessandro Cassinelli	02/04/2024
Redatto	Legal & Privacy	Alice Vanni	02/04/2024
Aggiornamento	Legal & Privacy	Claudia Amelia Urbano	23/09/2026

Aggiornamento

VERSIONE	DATA	NOTE
1.0	02/04/2024	Creazione documento
2.0	23/09/2026	Aggiornamento documento

PREMESSA

La presente Policy ha l'obiettivo di recepire, tempo per tempo e in coerenza con le caratteristiche del modello di business, le indicazioni in materia di profili etici definite a livello di Unione Europea e di Organizzazione per la Sicurezza e la Cooperazione in Europa (OCSE), con riferimento al governo dei modelli di intelligenza artificiale utilizzati da TESISQUARE (d'ora in avanti "Intelligenza Artificiale" o anche "IA").

In particolare, alla data di stesura del presente documento, le normative e linee guida di riferimento sono le seguenti:

1. OCSE, Raccomandazione del Consiglio sull'intelligenza artificiale del 22 maggio 2019 (OECD/Legal/0449, Recommendation of the Council on Artificial Intelligence);
2. Regolamento (UE) 2024/1689 – AI ACT entrato in vigore il 1° agosto 2024;
3. Regolamento (UE) 2026/1744 (Digital Omnibus on AI), entrato in vigore il 27 luglio 2026.

TESISQUARE riconosce l'importanza di far fronte alle sfide legate all'utilizzo dell'IA e di prendere in considerazione i temi etici che ne derivano. A tal riguardo, TESISQUARE monitora continuamente gli sviluppi normativi, anche a livello regolamentare e di linee guida, per un puntuale e tempestivo recepimento e adeguamento della propria normativa interna, ove ritenuto opportuno, , adeguando progressivamente le proprie procedure alle scadenze normative chiave (es. applicazione generale ad agosto 2026, operatività dei divieti assoluti a dicembre 2026 e obblighi per sistemi ad Alto Rischio a dicembre 2027).

Nei capitoli successivi sono descritti i principi ai quali TESISQUARE si ispira nell'approccio a tale tematica, distinguendo chiaramente le responsabilità connesse ai due ruoli operativi ricoperti dall'Azienda (Utilizzatore/Deployer e Fornitore/Provider)

1. Policy

TESISQUARE riconosce il potenziale trasformativo dell'Intelligenza Artificiale, ma è cosciente dei rischi che da questa possono derivare e pertanto si impegna a utilizzarla in modo etico, responsabile e sicuro per migliorare l'efficienza, l'innovazione e la qualità dei prodotti e servizi offerti ai propri clienti, e in ogni caso in conformità alla presente Policy.

TESISQUARE ha individuato due direttrici nell'utilizzo dell'IA:

1. **Efficienza dei processi interni:** TESISQUARE intende supportare i processi decisionali e produttivi utilizzando l'IA. Ad esempio, i software che utilizzano l'IA consentono di effettuare analisi ed estrazioni di dati in maniera più rapida e precisa rispetto ad analisi ed estrazioni manuali, possono supportare il lavoro del personale di TESISQUARE in operazioni ripetitive e standardizzate e possono anche aiutare i team di sviluppo di prodotto nella scrittura di codice sorgente (operando esclusivamente all'interno di ambienti aziendali strutturati e controllati, quali ad esempio Cursor Teams o Microsoft Copilot Enterprise).

2. **L'IA nei prodotti e servizi di TESISQUARE (ruolo di Fornitore – provider)**: TESISQUARE si pone l'obiettivo di sviluppare e commercializzare prodotti (software o algoritmi , quali ad esempio le soluzioni proprietarie AgentDoc, Cogito e Synapse) che sfruttano le potenzialità dell'Intelligenza Artificiale, allo scopo di migliorare i processi aziendali dei propri clienti e promuovere soluzioni digitali innovative. Per lo sviluppo di tali prodotti e servizi, TESISQUARE utilizza esclusivamente modelli di Intelligenza Artificiale forniti da partner tecnologici qualificati, i cui strumenti sono oggetto di licenza e vengono accuratamente selezionati e verificati. TESISQUARE si assicura che tali modelli siano conformi alla normativa vigente in materia di protezione dei dati personali (GDPR) e al Regolamento europeo sull'Intelligenza Artificiale (AI Act), nel rispetto dei principi di sicurezza, trasparenza, affidabilità e responsabilità.

Le applicazioni di IA utilizzate in TESISQUARE e sviluppate da TESISQUARE per i propri clienti saranno soggette a una valutazione continua per monitorare le prestazioni, l'equità e l'aderenza ai principi stabiliti dalla presente Policy. Eventuali problemi identificati saranno affrontati e corretti tempestivamente.

TESISQUARE promuove e garantisce l'alfabetizzazione all'IA del proprio personale, intesa dal Regolamento Omnibus (UE 2026/1744) come un obbligo di mezzi finalizzato a diffondere una consapevolezza adeguata sui rischi, sui limiti e sul corretto utilizzo delle tecnologie (Art. 4 AI Act).

2. Destinatari

La presente Policy è indirizzata a tutti i dipendenti di TESISQUARE e alle società collegate e/controllate di TESISQUARE S.p.A., nonché ai vari stakeholder di TESISQUARE che ne prenderanno visione e ne accetteranno i contenuti. Le disposizioni contenute nel presente Regolamento sono vincolanti e si applicano indistintamente a chiunque operi, a qualsiasi titolo e con qualsiasi tipologia contrattuale, all'interno del perimetro aziendale o nell'interesse dell'Azienda (inclusi dirigenti, collaboratori parasubordinati, lavoratori interinali, stagisti, consulenti esterni e fornitori di servizi).

3. Principi guida generali

Sia nell'utilizzo dell'IA per migliorare e rendere più efficienti i propri processi interni, sia nelle attività di sviluppo e commercializzazione di IA, TESISQUARE rispetta le seguenti linee guida.

Conformità alla legge. TESISQUARE **si impegna a rispettare tutte le leggi e le normative in vigore** riguardanti l'IA, garantendo la massima conformità e adattamento a eventuali aggiornamenti normativi. TESISQUARE opera nel pieno rispetto del Regolamento (UE) 2024/1689 (AI Act) e delle modifiche introdotte dal Regolamento (UE) 2026/1744 (Digital Omnibus). Il quadro normativo

adotta un approccio *risk-based* e impone obblighi ai fornitori ed agli sviluppatori di sistemi di IA in base ai diversi livelli di rischio: **rischio inaccettabile, rischio elevato, rischio limitato e rischio minimo o nullo**. TESISQUARE si impegna a conformarsi a tali disposizioni. Pertanto, TESISQUARE non utilizza e non sviluppa, a titolo di esempio, sistemi di IA che utilizzano tecniche subliminali che agiscono senza che una persona ne sia consapevole, sistemi di IA che sfruttano le vulnerabilità di uno specifico gruppo di persone, dovute all'età o alla disabilità fisica o mentale, al fine di distorcere materialmente il comportamento di una persona che appartiene a tale gruppo, sistemi di IA che consentono la valutazione o la classificazione dell'affidabilità delle persone fisiche per un determinato periodo di tempo sulla base del loro comportamento sociale o di caratteristiche personali o della personalità note o previste, sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico; sistemi di categorizzazione biometrica che utilizzano caratteristiche sensibili come genere, razza, etnia, cittadinanza, religione o orientamento politico, nonché sistemi per generare o manipolare contenuti intimi o sessualmente espliciti non consensuali (deepfakes). Per l'utilizzo e la commercializzazione di altri sistemi a rischio elevato, limitato o nullo, TESISQUARE si impegna a conformarsi agli obblighi stabiliti dall'AI ACT e della presente Policy.

***"L'uomo ha il controllo"* (Human-in-the-Loop: HITL) e principio di responsabilità**. L'IA è intesa da TESISQUARE come un semplice strumento. In qualsiasi momento, le persone possono decidere quando e come utilizzare i risultati forniti dallo strumento. È quello che accade, per esempio, quando una macchina aiuta gli umani nei compiti di classificazione. L'IA deve essere utilizzata come strumento di supporto per le decisioni umane, non come sostituto. Le decisioni importanti devono sempre prese da esseri umani. A tale principio è strettamente collegato il principio di responsabilità. **Gli output dell'IA possono supportare una decisione dell'uomo, ma non possono prendere il posto delle decisioni umane**. In applicazione del principio di sorveglianza umana, qualsiasi output o suggerimento prodotto da un'IA deve essere considerato una mera proposta di lavoro. Ciò significache gli output dell'IA devono sempre essere soggetti a supervisione da parte dei dipendenti addetti all'utilizzo di applicazioni IA. Ad esempio, l'utilizzo di sistemi di IA generativa per la scrittura di stringhe di codice sorgente non esonera lo sviluppatore dal verificare la correttezza, integrità e compatibilità del codice sviluppato; oppure, la generazione di immagini o post destinati ad un social network tramite sistemi di IA non esonera l'utilizzatore dal verificare che l'immagine o il post non violino diritti di proprietà intellettuale di terzi. Per le soluzioni proprietarie, la validazione umana deve avvenire attraverso le interfacce dedicate, quali la Validator GUI per AgentDoc e i meccanismi di feedback (Thumbs up/down) per Cogito e Synapse. I sistemi di IA sono spesso "black box" e gli output sono da utilizzare con grande prudenza.

4. Principi guida specifici relativi all'utilizzo di IA

TESISQUARE ritiene che l'IA possa contribuire a migliorare la qualità di alcuni processi interni e a renderli più efficienti, nel rispetto dei seguenti principi.

Confidenzialità e tutela del know how e della proprietà intellettuale di TESISQUARE e prevenzione dello "Shadow AI". I dati e le informazioni aziendali, e in particolare il codice sorgente dei software

TESISQUARE, sono un asset fondamentale per TESISQUARE. **È fatto divieto agli utilizzatori di riversare informazioni aziendali riservate di TESISQUARE all'interno di modelli di linguaggio aperti al pubblico** (come ad esempio le versioni gratuite di ChatGPT, Gemini o Claude). Al fine di prevenire il rischio di fughe di dati e vulnerabilità informatiche, il personale autorizzato deve svolgere le proprie attività esclusivamente all'interno degli ambienti protetti contrattualizzati da Tesisquare a livello Enterprise. Nell'interazione con gli strumenti di IA autorizzati, i Destinatari sono tenuti ad applicare le regole di prompting sicuro, astenendosi dall'inserire nei prompt dati personali identificativi, informazioni riservate o porzioni critiche di codice proprietario.

GDPR, tutela dei dati personali e garanzie giuslavoristiche. È fatto divieto agli utilizzatori di riversare dati personali all'interno di sistemi di IA, soprattutto se aperti al pubblico. Tali trattamenti di dati personali non sono infatti censiti all'interno delle informative privacy aziendali né all'interno del Registro dei trattamenti e sono pertanto da considerarsi illegittimi. Ad esempio, **è fatto divieto di effettuare tramite sistemi di IA estrazioni di dati relativi a dipendenti o clienti di TESISQUARE, o effettuare screening di curriculum tramite sistemi di IA**. A tal fine, nell'ambito della gestione delle risorse umane, Tesisquare vieta tassativamente l'adozione di provvedimenti individuali che incidano in modo significativo sulla vita lavorativa dei dipendenti o dei candidati basati unicamente su elaborazioni automatizzate. Qualsiasi atto aziendale adottato in assenza di un intervento umano effettivo e critico è da considerarsi giuridicamente nullo. È altresì vietata qualsiasi forma di profilazione psicologica, emotiva o comportamentale dei lavoratori, al fine di escludere la ri-qualificazione dei sistemi interni come sistemi ad Alto Rischio (Allegato III dell'AI Act).Ogni eccezione a tale divieto deve essere approvata da TESISQUARE, previa verifica da parte della Direzione Legale, in modo tale da effettuare le opportune valutazioni di impatto.

Trasparenza. L'utilizzo di sistemi di intelligenza artificiale per ottenere un determinato output (una slide, un'analisi, un report etc.) deve sempre essere dichiarato al proprio interlocutore. Ciò non significa che ogni singolo prompt ad un sistema di IA deve essere dichiarato; ad esempio, è possibile scrivere di proprio pugno un report interrogando di tanto in tanto un sistema di intelligenza artificiale su alcuni passaggi sui quali si hanno dubbi. Tuttavia, se il report è stato generato interamente da un sistema di IA, è fatto obbligo di segnalarlo, tenendo sempre a mente che la responsabilità finale del suo contenuto è sempre di colui che ha interrogato il sistema di IA per la produzione del report.

Prudenza. A causa dell'opacità dei processi interni delle reti neurali e dell'inaccessibilità di tutti i dati contemporaneamente trattati dai sistemi di IA basati sul deep learning, i sistemi di IA vengono talvolta definiti come "black box". Anche se il sistema di IA funziona perché restituisce output coerenti rispetto ai prompt, non sappiamo esattamente come raggiunge questi esiti o quali dati influenzano maggiormente le sue decisioni, a differenza dei programmi informatici tradizionali, dove tutto il codice è stato compilato in modo controllato e con ampio intervento da parte degli esseri umani. Questa circostanza impone agli utilizzatori di IA di **innalzare il livello di attenzione** ogni qualvolta si utilizzano sistemi di IA per la generazione di contenuti, documenti, analisi, report, perché l'output potrebbe violare diritti di terzi (si pensi al caso della generazione di stringhe di codice sorgente di proprietà di terzi, o la generazione di un'immagine di una persona da inserire

in una campagna di marketing che corrisponde ad una persona realmente esistente). In caso di dubbi, contattare la Direzione Legale.

5. Principi guida specifici relativi allo sviluppo e commercializzazione di sistemi di IA ai clienti di TESISQUARE

TESISQUARE si impegna a sviluppare e distribuire ai propri clienti sistemi di IA conformi alla legge (e in particolare alle direttive dell'AI ACT) e alle linee guida tempo per tempo definite dagli organismi nazionali e internazionali impegnati in materia di IA, e nel rispetto dei seguenti principi e secondo la filosofia della "compliance by design", inserendo barriere tecniche, logiche di trasparenza e sistemi di controllo umano direttamente all'interno dell'architettura software (es. tramite le soluzioni AgentDoc, Cogito e Synapse).

Uso responsabile dei dati del cliente. TESISQUARE è responsabile della custodia di una grande mole di dati dei propri clienti. L'utilizzo di tali dati per analisi avanzate mediante sistemi di IA avviene in modo **trasparente, dichiarato, conforme agli obblighi di confidenzialità e agli obblighi imposti dal GDPR e dalle altre leggi applicabili**. A tal fine, tutta l'infrastruttura di computazione e storage risiede all'interno del territorio dell'Unione Europea (Data Residency UE) e i dati dei clienti non vengono mai utilizzati per l'addestramento di modelli pubblici. TESISQUARE utilizza i dati del cliente in modo responsabile, affrontando volta per volta eventuali questioni legali ed etiche che si presentano.

Trasparenza. I sistemi di IA **sono progettati e sviluppati in modo tale da garantire che il loro funzionamento sia sufficientemente trasparente** da consentire agli utenti di interpretare l'output del sistema e utilizzarlo adeguatamente. TESISQUARE garantisce che i sistemi di IA siano progettati e sviluppati in modo tale che le persone fisiche siano informate del fatto di stare interagendo con un sistema di IA (in conformità all'obbligo di trasparenza ex Art. 50 dell'AI Act, tramite avvisi integrati nell'interfaccia e non disattivabili), a meno che ciò non risulti evidente dalle circostanze e dal contesto di utilizzo.

Tracciabilità ed explainability. TESISQUARE progetta e distribuisce sistemi di IA con capacità che consentono la **registrazione automatica degli eventi (log)** durante il loro funzionamento, assicurandone la conservazione sicura per un periodo minimo di sei mesi. Predispone inoltre **adeguata documentazione tecnica** che ne descriva il funzionamento e le modalità di addestramento.

Sicurezza. TESISQUARE progetta e distribuisce sistemi di IA in modo tale da conseguire, alla luce della loro finalità prevista, un adeguato livello di **accuratezza, robustezza e cybersicurezza** e da operare in modo coerente con tali aspetti durante tutto il loro ciclo di vita, implementando soluzioni efficaci contro minacce specifiche dell'IA come la prompt injection.

Responsabilità di filiera e contratti con terzi (art. 25). Nello sviluppo delle proprie soluzioni, TESISQUARE stipula accordi scritti di filiera con i fornitori dei modelli per finalità generali (GPAI) a monte, garantendo la ricezione delle informazioni tecniche necessarie e mitigando i rischi

sistemici. Parallelamente, nei contratti stipulati con soggetti esterni (consulenti, fornitori) che interagiscono con i sistemi aziendali, TESISQUARE dispone l'inserimento obbligatorio di clausole in conformità all'art. 25 dell'AI Act.

6. Revisione periodica

Il presente Regolamento è sottoposto a riesame e aggiornamento ordinario con cadenza annuale, a cura dell'Ufficio Legal in stretto coordinamento con il CISO, l'AI Competence Center e il DPO per assicurare che rimanga allineata agli sviluppi tecnologici, etici e normativi in evoluzione nell'ambito dell'IA.

7. Conseguenze dei controlli

La violazione delle prescrizioni e dei divieti stabiliti dal presente Regolamento costituisce illecito disciplinare e inosservanza dei doveri contrattuali. Tali condotte saranno sanzionate in conformità con le procedure previste dal Contratto Collettivo Nazionale di Lavoro (CCNL) applicabile. In caso di violazione dei principi della presente Policy, TESISQUARE avrà diritto di procedere nei confronti del soggetto interessato contestando un inadempimento contrattuale nelle modalità previste dalla legge e dal contratto stesso. Qualora le violazioni commesse integrino fattispecie di reato o comportamenti idonei a comportare la responsabilità amministrativa dell'Azienda, le relative contestazioni saranno coordinate con il sistema disciplinare del Modello di Organizzazione e Gestione ex D.Lgs. 231/2001 (MOG 231).