

POLITICA SULL'USO DEGLI STRUMENTI DI IA

Versione 1.0 del 07/10/2026

INDICE

1. Introduzione 3

1.1. Contesto di riferimento 3

1.2. Riferimenti normativi 3

1.2.1. Normativa cogente 3

1.2.2. Normativa interna 3

1.3. Obiettivi 5

1.4. Definizioni e terminologia 5

2. Ambito di applicazione 8

3. Principi generali dell'intelligenza artificiale 9

3.1. Robustezza, accuratezza e sicurezza dei sistemi di IA 9

3.2. Protezione dei dati personali e della proprietà intellettuale 9

3.3. Human Oversight 10

3.3.1. Human in the Loop 10

3.4. Trasparenza e spiegabilità 10

3.5. Equità e non discriminazione 11

4. Processo per lo sviluppo e l'utilizzo responsabile dei Sistemi di IA 12

4.1. Documentazione, tracciabilità e gestione del ciclo di vita dei sistemi di IA 12

5. Segnalazioni 12

6. Formazione in materia di IA 13

7. Revisione della politica sull'IA 13

1. Introduzione

1.1. Contesto di riferimento

L'intelligenza artificiale (di seguito "IA") rappresenta un fattore abilitante per l'innovazione, l'efficienza operativa e la qualità dei servizi offerti dal Gruppo TAS (di seguito anche "TAS"). L'evoluzione delle tecnologie generative, predittive e analitiche apre nuove opportunità nel supporto allo sviluppo software, nella gestione dei documenti, nell'ottimizzazione dei processi e nel miglioramento dell'esperienza utente.
Parallelamente, l'adozione di tali tecnologie introduce rischi rilevanti in termini di sicurezza delle informazioni, proprietà intellettuale, protezione dei dati, accuratezza dei risultati e affidabilità dei sistemi. La presente Politica dell'IA (di seguito "Politica") definisce i principi che guidano l'utilizzo, lo sviluppo e l'integrazione responsabile dell'IA nel Gruppo TAS. Essa fornisce un quadro di riferimento unitario, coerente con la normativa europea e nazionale in materia, assicurando un approccio prudente, etico e orientato alla tutela degli asset informativi e della reputazione aziendale. L'obiettivo è promuovere un uso dell'IA che amplifichi le competenze delle persone, salvaguardi la riservatezza dei dati, garantisca comportamenti trasparenti e mantenga elevati standard di qualità e sicurezza lungo tutto il ciclo di vita dei sistemi.

1.2. Riferimenti normativi

1.2.1. Normativa cogente

- Regolamento (UE) 2024/1689 (AI Act);
- Regolamento (UE) 2016/679 (GDPR);
- Direttiva (UE) 2022/2555 (NIS2);
- Regolamento (UE) 2022/2554 (DORA);
- L. 300/1970 (Statuto dei Lavoratori, in particolare Art. 4);
- L. 633/1941 e Direttiva (UE) 2019/790 (Copyright);
- D.Lgs. 231/2001 (Disciplina della responsabilità amministrativa delle persone giuridiche);
- Normative tecniche e di settore in materia di sicurezza delle informazioni, tutela della proprietà intellettuale e classificazione dei dati;

1.2.2. Normativa interna

- Regolamento aziendale e codice disciplinare
- Codice Etico aziendale
- Modello Organizzativo e di Gestione ai sensi del D.Lgs231/01
- SQPRC052-Adozione e gestione dei sistemi di Intelligenza Artificiale
- SQPRC001-Gestione delle informazioni documentate
- SQPRC002-Gestione della formazione
- SQPRC012-Progettazione e sviluppo di soluzioni software
- SQPRC013-Pianificazione, erogazione e monitoraggio dei servizi

- SQPRC019-Predisposizione ed esecuzione dei test
- SQPRC022-Assistenza e manutenzione delle soluzioni informatiche realizzate
- SQPRC031-Security incident management
- SQPRC034-Privacy ed adeguamenti normativi
- SQPRC035-BIA e risk assessment
- SQPRC046-Pianificazione e gestione delle scansioni di sicurezza
- SQPRC047-Identificazione e gestione delle vulnerabilità
- SQPRC044-Whistleblowing-Altre società del Gruppo TAS
- SQPRC045-Whistleblowing-TAS

1.3.Obiettivi

La Politica persegue i seguenti obiettivi:

- promuovere un utilizzo dell'IA sicuro, etico e responsabile atto a favorire la diffusione di competenza e consapevolezza tra il personale e a prevenire - per quanto possibile - errori, distorsioni o comportamenti inattesi;
- tutelare i dati personali, la proprietà intellettuale e il patrimonio informativo del Gruppo TAS;
- garantire che l'IA supporti le competenze umane senza sostituirsi ad esse;
- assicurare la piena conformità dei processi aziendali alle normative europee e nazionali applicabili, adottando un approccio basato sul rischio in linea con l'AI Act, il GDPR e i requisiti di sicurezza delle reti e dei sistemi informativi (DORA e NIS2);
- garantire la trasparenza, la tracciabilità e la spiegabilità delle soluzioni basate sull'IA, rafforzando la fiducia dei clienti e degli stakeholder verso i prodotti e i servizi erogati dal Gruppo;
- indirizzare l'innovazione tecnologica verso il miglioramento continuo dell'efficienza operativa e della qualità degli artefatti prodotti (es. software, documentazione), mantenendo in ogni fase l'obbligo inderogabile del controllo umano sui processi decisionali;
- promuovere lo sviluppo e l'adozione di sistemi di IA che rispettino i criteri di sostenibilità (ESG) e i valori del Codice Etico aziendale, ripudiando qualsiasi forma di discriminazione algoritmica o violazione dei diritti fondamentali.

1.4. Definizioni e terminologia

Dato Personale (o Dati Personali)	Qualsiasi informazione riferita a una persona fisica identificata o identificabile. È considerata identificabile la persona che può essere riconosciuta, direttamente o indirettamente, mediante elementi quali il nome, un numero identificativo, dati relativi alla posizione, un identificativo online o altri fattori specifici della sua identità fisica, fisiologica, genetica, psicologica, economica, culturale o sociale.
Destinatario	Soggetto che subisce o può subire gli effetti generati dal Sistema di IA, anche in assenza di un'interazione diretta con esso. Tale soggetto può coincidere, in determinate circostanze, con l'Utenza.
Incidente Grave/Disastroso	Evento che comporta un impatto grave /disastroso (secondo la classificazione aziendale di cui alla procedura SQPRC035 BIA e Risk Assessment), sulla sicurezza delle persone, sulla

	tutela dei dati personali, sull'affidabilità dei processi aziendali o sul rispetto dei diritti fondamentali. Ai sensi dell'AI Act, un incidente è considerato grave quando provoca, o rischia ragionevolmente di provocare, danni rilevanti a persone fisiche, perdite o compromissioni significative di dati, oppure effetti lesivi su beni, attività o procedimenti critici.
Modello di IA	La componente algoritmica addestrata su dati che consente a un Sistema di IA di produrre un certo tipo di output.
Pratiche di IA vietate	Categorie di utilizzo dell'intelligenza artificiale espressamente proibite dall'AI Act in quanto considerate contrarie ai diritti fondamentali, alla sicurezza o alla dignità della persona. Rientrano tra le pratiche vietate, a titolo esemplificativo, i sistemi progettati per manipolare il comportamento umano attraverso tecniche subliminali o sfruttando vulnerabilità specifiche; i sistemi di social scoring applicati a persone fisiche; l'utilizzo di tecnologie che consentano il riconoscimento biometrico in tempo reale in spazi accessibili al pubblico al di fuori dei casi consentiti; nonché qualsiasi applicazione che comporti un rischio eccessivo per la sicurezza pubblica o l'integrità dei processi democratici.
Rischio IA	Potenziale effetto negativo derivante dall'uso di un Sistema di IA, inclusi rischi per la sicurezza dei dati, la qualità dell'output, la protezione della proprietà intellettuale o l'impatto su persone e processi.
Sistema di Intelligenza artificiale (IA)	Un sistema basato su modelli algoritmici o statistici capace di generare output quali previsioni, raccomandazioni, contenuti o decisioni che influenzano ambienti fisici o virtuali.
Sistema di IA generativa	Sistema di IA progettato per generare contenuti nuovi e originali — come testo, codice, immagini o analisi — sulla base di modelli addestrati su grandi quantità di dati.

IA ad alto rischio / IA a rischio limitato	Categorie di rischio previste dall'AI Act, che classificano i sistemi di IA in base al potenziale impatto sui diritti, sulla sicurezza o sui processi critici. A livelli di rischio diversi corrispondono misure di tutela proporzionate.
Human Oversight (Supervisione Umana)	La capacità, per le persone, di monitorare, comprendere e intervenire sui risultati generati da un Sistema di IA al fine di garantirne l'uso sicuro ed efficace.
Human in the Loop (HITL)	Modalità di utilizzo dell'IA in cui il contributo umano è parte integrante del processo, attraverso la verifica, la correzione o la convalida degli output generati dal modello prima del loro utilizzo operativo.
Bias algoritmico	Deviazione non intenzionale presente nei dati o nei modelli che può tradursi in risultati distorti o discriminatori.
Documentazione tecnica	Insieme minimo di informazioni necessarie a descrivere il funzionamento, le caratteristiche, le modalità d'uso e gli output di un Sistema di IA, utile per garantire trasparenza, controllo e corretta manutenzione.
Ciclo di vita del Sistema di IA	L'insieme delle fasi che compongono l'esistenza di un sistema di IA, dalla valutazione preliminare del caso d'uso allo sviluppo, validazione, utilizzo, monitoraggio e aggiornamento.
Fallback (o meccanismo di disattivazione)	Capacità di sospendere o sostituire l'utilizzo del Sistema di IA quando l'output risulti inattendibile, inadeguato o rischioso, garantendo continuità operativa attraverso procedure alternative.

2. Ambito di applicazione

La seguente Politica si applica:

- a tutte le società del Gruppo TAS che utilizzano o implementano sistemi di IA;
- a tutti i dipendenti, collaboratori, consulenti e fornitori autorizzati ad accedere a strumenti o modelli di IA di proprietà di TAS;
- a ogni utilizzo, diretto o indiretto, di piattaforme, servizi, modelli o strumenti che incorporano funzioni di IA, generativa o non generativa.

Essa disciplina esclusivamente i principi e non le modalità operative, che sono regolamentate nelle specifiche procedure aziendali.

Il Gruppo TAS riconosce che i sistemi di IA presentano livelli di rischio differenti, in conformità al quadro normativo europeo[1]. L'impiego di soluzioni di IA comporta pertanto l'adozione di misure proporzionate al livello di rischio, distinguendo tra sistemi a rischio limitato, moderato o elevato.

[1] Così come definito nel Regolamento (UE) 2024/1689 (AI Act).

3. Principi generali dell'intelligenza artificiale

L'adozione dell'intelligenza artificiale all'interno del Gruppo TAS è guidata da un insieme di principi fondamentali che orientano ogni attività connessa al suo sviluppo, al suo impiego e alla sua integrazione nei processi aziendali. Tali principi rappresentano un orientamento stabile e trasversale, volto a garantire che l'utilizzo dell'IA avvenga in modo sicuro, etico, trasparente e compatibile con gli standard di qualità che contraddistinguono l'operatività del Gruppo.

3.1. Robustezza, accuratezza e sicurezza dei sistemi di IA

La sicurezza delle informazioni e dei sistemi rappresenta un requisito essenziale per ogni applicazione di intelligenza artificiale. L'IA deve essere progettata e utilizzata in modo tale da garantire livelli adeguati di safety *e* cybersecurity*,* prevenendo rischi che possano compromettere l'integrità dei dati, la continuità operativa o la qualità dei processi aziendali.

La robustezza *e* l'accuratezza costituiscono elementi fondamentali di questo principio. La robustezza esprime la capacità del modello di mantenere comportamenti affidabili e coerenti anche quando è esposto a variazioni, rumore, input imprevisti o condizioni non perfettamente aderenti al contesto di addestramento. L'accuratezza riguarda la correttezza, la pertinenza e la coerenza dei risultati generati rispetto allo scopo perseguito.

Tutto il personale deve essere consapevole che i modelli di IA, pur avanzati, possono produrre output incompleti, errati o distorti.

È pertanto necessario adottare un approccio critico e prudente, verificando la fondatezza dei risultati e applicando, quando opportuno, controlli aggiuntivi o correzioni manuali. L'obiettivo è assicurare che l'utilizzo dell'IA non introduca rischi non controllati e che i sistemi impiegati contribuiscano in modo affidabile, sicuro e trasparente alla qualità delle attività aziendali.

3.2. Protezione dei dati personali e della proprietà intellettuale

Il patrimonio informativo del Gruppo TAS – che comprende dati personali, codici sorgente, documentazione tecnica, logiche applicative e dati dei clienti – rappresenta un asset strategico. Ogni interazione con sistemi di IA deve essere conforme ai requisiti del GDPR, alle politiche interne di classificazione dei dati e alle regole di tutela della proprietà intellettuale.

È vietato condividere informazioni riservate, confidenziali o sensibili con piattaforme di IA che non offrano garanzie adeguate in termini di protezione, conservazione e trattamento dei dati. Il principio di minimizzazione impone di limitare lo scambio di informazioni al minimo necessario, utilizzando per le attività lavorative gli strumenti aziendali resi disponibili.

TAS, nella scelta degli strumenti di IA, subordina il trasferimento di dati verso provider soggetti a giurisdizioni extra-UE (in particolare USA) a rigorosi controlli. Oltre alla verifica dell'adesione a decisioni di adeguatezza o alla firma di SCC, l'Azienda valuta il rischio di ingerenza da parte di autorità governative estere disciplinate da normative sulla sorveglianza. Ove necessario, l'Azienda impone l'adozione di misure tecniche supplementari (es. cifratura) a tutela degli interessati.

3.3. Human Oversight

Il Gruppo TAS attribuisce un ruolo centrale alla supervisione umana nel processo di utilizzo dell'IA. Ogni output deve essere esaminato, validato e contestualizzato, in modo da garantire che i risultati generati siano coerenti, accurati e adeguati allo scopo. La supervisione umana previene interpretazioni errate, riduce il rischio di errori e assicura che l'IA rimanga uno strumento di supporto e non un sostituto del giudizio umano.

3.3.1. Human in the Loop

In coerenza con le procedure interne e con i principi promossi dal Gruppo TAS, il concetto di Human in the Loop rappresenta una declinazione concreta del controllo umano sull'intelligenza artificiale. Esso prevede che l'intervento dell'uomo non sia soltanto eventuale o residuale, ma parte integrante del processo di utilizzo dell'IA, con un ruolo attivo e determinante nel valutare, confermare o correggere i risultati generati.

L'approccio Human in the Loop implica che ogni output dell'IA venga sottoposto a una verifica qualitativa e funzionale prima di essere utilizzato in maniera definitiva nei processi aziendali. Ciò significa che le persone mantengono il controllo sulle decisioni che l'IA può influenzare, garantendo che le analisi effettuate dai modelli o i contenuti generati siano coerenti, accurati e pienamente rispondenti alle aspettative organizzative. Tale principio garantisce il pieno rispetto dell'Art. 22 del GDPR, assicurando agli interessati il divieto di essere sottoposti a decisioni basate unicamente su trattamenti automatizzati che producano effetti giuridici

Questo principio assume particolare rilievo nei contesti in cui l'IA supporta attività tecniche o documentali, come lo sviluppo del codice, la redazione di testi, la classificazione di contenuti o l'elaborazione di informazioni che presentano un potenziale impatto operativo. Nei casi in cui l'IA generi porzioni di codice o rielaborazioni testuali, il personale competente è chiamato a esaminare attentamente tali risultati, integrandoli con il proprio giudizio professionale e validandoli prima che siano incorporati in sistemi, processi o documentazione aziendale.

Nell'ambito del principio di Human in the Loop, il personale mantiene la possibilità di intervenire, correggere o sostituire il risultato prodotto dall'IA qualora questo risulti inadeguato, incompleto o potenzialmente dannoso. Ciò include la capacità di sospendere l'utilizzo dello strumento o di ricorrere a modalità alternative di esecuzione dell'attività, attuando forme di "fallback" che assicurino continuità operativa e qualità del processo anche in presenza di comportamenti inattesi del modello.

3.4.Trasparenza e spiegabilità

L'uso dell'IA deve essere improntato alla trasparenza: i dipendenti devono essere consapevoli delle finalità, delle logiche generali e dei limiti degli strumenti utilizzati. Quando necessario, devono essere adottate soluzioni che permettano di comprendere in modo adeguato le ragioni che hanno condotto a un certo risultato, così da consentire una valutazione critica e informata.

La spiegabilità costituisce un elemento essenziale di tale trasparenza. Essa implica la capacità, per l'utente, di comprendere in termini chiari e comprensibili il funzionamento delle principali logiche del modello e i fattori che hanno influenzato l'output generato. Una spiegabilità adeguata rafforza la fiducia, permette di identificare eventuali errori o bias e consente al personale di esercitare un controllo consapevole sui risultati prodotti dall'IA.

Laddove applicabile, TAS si impegna inoltre a garantire che anche i clienti siano informati in modo chiaro e comprensibile dell'utilizzo di sistemi di Intelligenza Artificiale nei servizi e nei prodotti offerti, in coerenza con i principi di trasparenza, correttezza e con le normative vigenti.

3.5. Equità e non discriminazione

L'intelligenza artificiale deve essere utilizzata in modo da evitare trattamenti ingiustificati o effetti discriminatori, intenzionali o non intenzionali. Quando il caso d'uso lo richiede, è opportuno dedicare attenzione alla qualità, alla rappresentatività e all'equilibrio dei dati utilizzati, così da prevenire distorsioni che possano riflettersi sui risultati generati.

Il Gruppo TAS promuove un approccio basato sulla correttezza e sull'imparzialità, richiedendo che eventuali bias o anomalie rilevate siano affrontati con tempestività, adottando misure correttive idonee a garantire l'equità dei processi supportati dall'IA.

4. Processo per lo sviluppo e l'utilizzo responsabile dei Sistemi di IA

L'impiego di strumenti di intelligenza artificiale deve avvenire con senso di responsabilità, consapevolezza tecnica e piena aderenza ai principi enunciati nella presente Politica. In particolare, TAS promuove un approccio che privilegi l'utilizzo di soluzioni aziendali o comunque di piattaforme che offrano adeguate garanzie di protezione dei dati e di tutela del patrimonio informativo. L'utilizzo di strumenti gratuiti o pubblicamente accessibili è ammesso solo quando si ha la certezza che le informazioni trattate non contengano elementi riservati o confidenziali, né dati personali o porzioni di codice proprietario.

Ogni interazione con sistemi di IA deve essere condotta in modo da evitare la divulgazione involontaria di informazioni sensibili. Ciò implica che la selezione degli strumenti non possa basarsi esclusivamente sull'intuitività o sulla comodità d'uso, ma debba considerare con priorità i rischi correlati alla conservazione dei dati, alle modalità di trattamento da parte del fornitore e alle possibili implicazioni contrattuali.

Nel contesto dello sviluppo software, il ricorso all'IA può rappresentare un valido aiuto per accelerare le attività, individuare errori o generare soluzioni alternative; tuttavia, il codice prodotto non può essere accettato acriticamente né introdotto nei progetti senza una revisione tecnica approfondita. Gli sviluppatori sono chiamati a verificare la correttezza logica del codice, la sua conformità agli standard interni e la compatibilità delle licenze associate agli strumenti utilizzati. Il ricorso all'IA non deve mai condurre alla perdita di controllo sugli artefatti software né alla compromissione della qualità del prodotto finale.

Analogamente, per quanto riguarda la gestione documentale, è essenziale valutare attentamente quali contenuti siano idonei a essere elaborati tramite strumenti di IA. I testi generici o privi di informazioni riservate possono essere trattati con maggiore flessibilità, mentre la documentazione classificata richiede un livello di protezione più elevato e non può essere condivisa con strumenti che non garantiscano adeguati livelli di sicurezza. Il personale è pertanto tenuto a effettuare una valutazione preventiva del contenuto prima di utilizzarlo all'interno di strumenti di IA.

TAS adotta un processo basato sul rischio per lo sviluppo, l'integrazione e l'utilizzo dei sistemi di IA.

Le modalità di valutazione preliminare, verifica di conformità, approvazione e monitoraggio sono disciplinate dalla procedura SQPRC052-Adozione e gestione dei sistemi di Intelligenza Artificiale e dalle relative istruzioni operative.

4.1. Documentazione, tracciabilità e gestione del ciclo di vita dei sistemi di IA

TAS riconosce l'importanza della tracciabilità e della documentazione nell'utilizzo dei sistemi di IA, favorendo una gestione responsabile del ciclo di vita dei modelli per garantire la ricostruibilità dei processi decisionali, secondo quanto disciplinato dalle procedure aziendali.

5. Segnalazioni

Un uso maturo e responsabile dell'intelligenza artificiale implica la capacità di riconoscere, intercettare e gestire tempestivamente anomalie o vulnerabilità.

Il personale è tenuto a segnalare senza ritardo, secondo quanto definito dalla procedura SQPRC052-Adozione e gestione dei sistemi di Intelligenza Artificiale, qualsiasi comportamento inatteso, bias o

rischio per la sicurezza e la riservatezza dei dati. Qualora la segnalazione riguardi situazioni che comportano violazioni del Codice Etico aziendale o condotte illecite o potenziali reati ai sensi del D.Lgs231/01 commessi tramite strumenti di IA, il personale deve utilizzare i canali whistleblowing adottati dall'azienda e definiti dalle procedure SQPRC044-Whistleblowing-Altre società del Gruppo TAS e SQPRC045-Whistleblowing-TAS, predisposte a garantire le necessarie tutele di riservatezza previste dalla normativa vigente.

Il mancato rispetto dei presenti principi e l'omessa segnalazione di incidenti secondo i canali aziendali predisposti costituiscono violazioni sanzionabili ai sensi del Regolamento aziendale e codice disciplinare.

6. Formazione in materia di IA

La corretta adozione dell'IA richiede che il personale disponga di un livello adeguato di conoscenza dei rischi e delle opportunità associati a tale tecnologia. TAS adotta pertanto, in ottemperanza all'Articolo 4 del Regolamento UE 2024/1689 (AI Act), iniziative di formazione mirate a favorire l'utilizzo competente e informato degli strumenti di IA, fornendo indicazioni sui principi da rispettare, sulle modalità corrette di interazione e sugli strumenti approvati per l'uso aziendale.

TAS, secondo quanto definito dalla procedura SQPRC052-Adozione e gestione dei sistemi di Intelligenza Artificiale, promuove iniziative di formazione volte a:

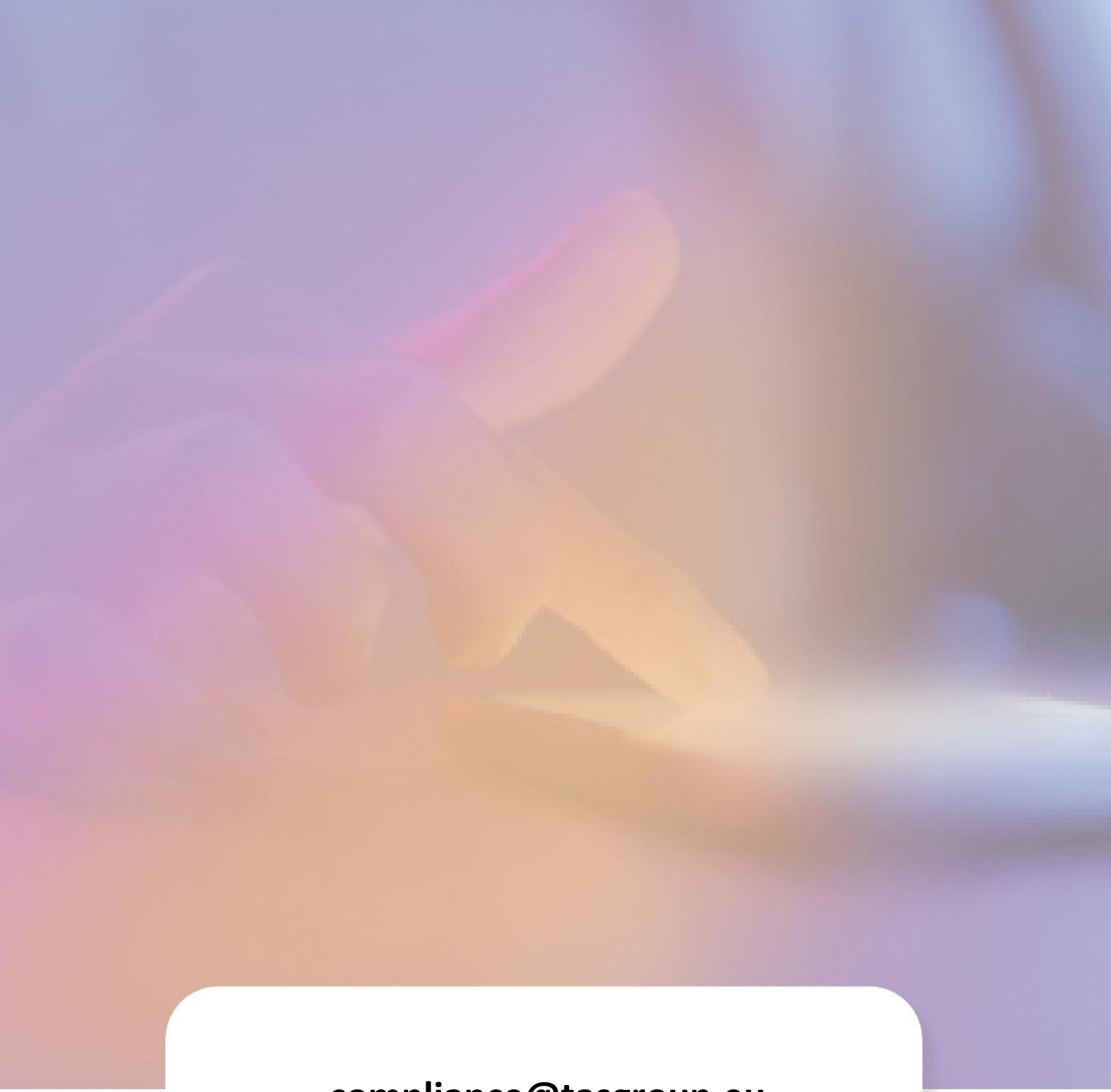
- accrescere la consapevolezza sui rischi e le opportunità dell'IA;
- favorire un utilizzo competente e critico degli strumenti;
- fornire indicazioni sugli strumenti approvati e sulle corrette modalità d'uso;
- diffondere la conoscenza delle procedure interne e delle normative applicabili.

La formazione è calibrata in base a ruoli, competenze e casi d'uso, e viene pianificata e gestita dall'Ufficio Formazione secondo quanto definito dalla procedura SQPRC002 Gestione della formazione.

7. Revisione della politica sull'IA

La presente Politica è soggetta a revisione almeno annuale e a revisione straordinaria qualora ne emerga l'esigenza, sia a seguito di aggiornamenti delle normative vigenti, sia per eventi che mutino il profilo di rischio (ad esempio non esaustivo introduzione strutturale di nuovi strumenti di IA, eventi geopolitici che possono portare a rivalutare gli strumenti adottati, eventi/segnalazioni derivanti dall'utilizzo operativo dell'IA nei processi aziendali, ecc…).

Le eventuali modifiche sono gestite secondo quanto definito dalla procedura SQPRC001-Gestione delle informazioni documentate del sistema di gestione.



compliance@tasgroup.eu