# Politica per un uso etico e responsabile dell'Intelligenza Artificiale

Regolamento (UE) 2024/1689 (AI Act)




Rev. 1.2 del 31 luglio 2026

# Sommario

Glossario ..... 4
1 Politica per l'utilizzo dell'Intelligenza Artificiale Gruppo Links ..... 4
2 Scopo e ambito di applicazione ..... 5
2.1 Ambito di applicazione ..... 5
3 Definizioni ..... 5
4 Riferimenti normativi ..... 6
5 Principi generali ..... 7
6 Governance dell'IA ..... 7
6.1 Responsabile IA (Chief Artificial Intelligence Officer - CAIO) e Comitato AI ..... 8
6.2 Registro dei Sistemi IA ..... 9
7 Ambiti di utilizzo autorizzati ..... 10
8 Rapporti con i Clienti ..... 11
8.1 Principi generali ..... 11
8.2 Comunicazione e policy AI del Cliente ..... 11
8.3 Strumenti, ambienti e registri ..... 12
8.4 Ruolo di Links ai sensi dell'AI Act ..... 12
8.5 Dati, codice e documentazione del Cliente ..... 13
8.6 Vincoli sopravvenuti ..... 13
9 Condizioni d'utilizzo ed utilizzi vietati o ad alto rischio ..... 13
9.1 Condizioni generali per tutti gli ambiti di utilizzo ..... 13
9.2 Divieti assoluti ..... 13
9.3 Utilizzi ad alto rischio (richiedono autorizzazione del CAIO) ..... 14
9.4 Informazioni che NON devono essere caricate su IA generativa pubblica ..... 14
10 Regole operative generiche per l'utilizzo dell'IA ..... 15
10.1 Utilizzo di IA Generativa ..... 15
10.2 Adozione degli strumenti IA nei progetti e nelle attività ..... 15
10.3 Configurazione obbligatoria ..... 16
10.3.1 Procedura operativa ..... 16
10.4 Supervisione umana obbligatoria ..... 17
10.5 Documentazione e tracciabilità ..... 17
10.6 Classificazione ed etichettatura dei contenuti generati con IA ..... 17

10.7 Workflow agentici ..... 18
10.8 Telemetria e tracciature (Logging) ..... 18
11 Trattamento dei dati e Privacy ..... 19
11.1 Tipologie di dati trattati con l'uso dell'IA ..... 19
11.2 Principi relativi alla Privacy e al GDPR nell'uso dell'IA ..... 20
11.3 Informativa agli interessati ..... 21
11.4 Diritto di opposizione (Art. 22 GDPR) ..... 21
11.5 Data Protection Impact Assessment (DPIA) ..... 21
11.6 Anonimizzazione e pseudonimizzazione ..... 21
12 Sicurezza e Cybersecurity ..... 22
12.1 Sicurezza dei sistemi IA ..... 22
12.2 Gestione delle vulnerabilità ..... 22
12.3 Supply Chain Security ..... 22
13 Diritti e tutele dei lavoratori ..... 22
13.1 Diritto all'informazione ..... 22
13.2 Diritto alla spiegazione ..... 23
13.3 Diritto di contestazione ..... 23
13.4 Canali di segnalazione ..... 23
13.5 Modalità di segnalazione ..... 23
13.6 Garanzie ..... 23
13.7 Tutela dal controllo a distanza (Art. 4 Statuto dei Lavoratori) ..... 24
14 Formazione e sensibilizzazione ..... 24
14.1 Programma formativo obbligatorio ..... 24
14.2 Aggiornamento continuo ..... 25
15 Monitoraggio, Audit e revisione ..... 25
15.1 Monitoraggio continuo ..... 25
15.2 Audit periodici ..... 25
15.3 Valutazione dei Bias ..... 25
15.4 Revisione della Policy ..... 26
16 Gestione delle violazioni ..... 26
16.1 Classificazione delle violazioni ..... 26
16.2 Sanzioni disciplinari ..... 26

16.3 Procedimento ..... 27
16.4 Obbligo di notifica ..... 27
17 Disposizioni finali .....27
17.1 Clausola di adeguamento normativo..... 27
17.2 Disposizioni attuative..... 27

# Glossario

La tabella seguente riporta il significato degli acronimi utilizzati nel presente documento, coerenti con la Struttura Organizzativa Links Group.

| Acronimo | Significato |
|---|---|
| CAIO | Chief Artificial Intelligence Officer |
| CISO | Chief Information Security Officer |
| DPO | Responsabile della Protezione dei Dati |
| HCC | Head of Competence Center |
| HRL | People and Culture Lead |
| HRO | People and Culture |
| IM | Incident Manager |
| LEG | Legal |
| PL | Project Lead (o Responsabile di Progetto) |
| PRO | Procurement |

# 1 Politica per l'utilizzo dell'Intelligenza Artificiale Gruppo Links

In **Links Management and Technology S.p.A.** ascoltiamo e innoviamo per disegnare il futuro digitale delle organizzazioni. Questo è il nostro purpose, quello per cui ogni giorno ci impegniamo. I nostri servizi e le nostre soluzioni contribuiscono a creare valore nella trasformazione digitale di banche e istituti finanziari, pubbliche amministrazioni e imprese.

**Links** è Parent Company di un Gruppo di aziende che unisce expertise per garantire soluzioni digitali Tailor-Made costruite e sviluppate sui Requirement del cliente con l'obiettivo di costruire e consolidare partnership di valore.

**Links** è fortemente votata allo sviluppo di soluzioni in modalità "Chiavi in mano" e all'erogazione di servizi di "System Integration", di "Cloud Computing" di "Application

Maintenance", di presidio applicativo per la manutenzione applicativa ordinaria, di **Cybersecurity e protezione dei dati personali,** sia **On Premise,** che **in Cloud**.

Data la natura delle proprie attività, **Links** considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo e un fattore di valenza strategica facilmente trasformabile in vantaggio competitivo, ponendo particolare attenzione ai temi riguardanti la sicurezza durante il ciclo di vita di progettazione e sviluppo dei propri prodotti e l'erogazione dei propri servizi, che devono essere ritenuti un bene primario dell'azienda.

Ciò premesso, Il Gruppo **Links** intende adottare le misure, sia tecniche che organizzative, necessarie a garantire al meglio l'integrità, la riservatezza e la disponibilità sia del patrimonio informativo aziendale e del Gruppo, sia di quello affidato dai propri Clienti in conformità alle prescrizioni legali o regolamentari, nonché gli obblighi contrattuali relativi alla sicurezza.

Con l'introduzione dell'**Intelligenza Artificiale (IA)** nei processi produttivi, il **Gruppo Links** si trova davanti a nuove sfide, sia per la sicurezza delle informazioni, sia per la tutela dei lavoratori e del proprio ingegno.

# 2 Scopo e ambito di applicazione

La presente Policy disciplina l'utilizzo di sistemi e strumenti di **Intelligenza Artificiale** per tutte le società del **Gruppo Links**, con l'obiettivo di:

- Garantire un impiego responsabile, trasparente ed etico dell'IA;
- Tutelare i diritti fondamentali dei lavoratori e delle persone coinvolte;
- Assicurare la conformità alla normativa europea e nazionale vigente;
- Promuovere l'innovazione nel rispetto della dignità umana e della sicurezza.

## 2.1 Ambito di applicazione

Questa Policy si applica a:

- Tutti i dipendenti, collaboratori e consulenti di Links e alle Società del Gruppo Links, in tutte le sedi del Gruppo;
- Tutti i sistemi di IA utilizzati o sviluppati dal Gruppo Links;
- Tutti i processi aziendali che coinvolgono strumenti di IA;
- Fornitori e partner che trattano dati per conto delle società del Gruppo Links, utilizzando IA.

# 3 Definizioni

- **Agente IA (Sistema di IA agentico):** sistema di IA in grado di pianificare ed eseguire sequenze di azioni con autonomia operativa, anche interagendo con strumenti, dati e

sistemi esterni tramite Componenti di integrazione IA e nell'ambito di architetture multi-agente.

- **Bias Algoritmico:** distorsione sistematica negli output dell'IA derivante da dati o modelli non bilanciati.
- **Componenti di integrazione IA:** elementi che estendono le capacità di un sistema di IA, quali, a titolo esemplificativo e non esaustivo, Tool e funzioni richiamabili (Tool Calling), connettori e server MCP (Model Context Protocol), Skill, istruzioni di sistema (System Prompt) e basi di conoscenza per il grounding delle risposte (RAG – Retrieval-Augmented Generation).
- **Dato**: qualsiasi rappresentazione digitale di atti, fatti o informazioni e qualsiasi raccolta di tali atti, fatti o informazioni, anche sotto forma di registrazione sonora, visiva o audiovisiva.
- **Gruppo Links:** il Gruppo è composto dalle aziende Links Management and Technology S.p.A., Nexus Advanced Technologies S.r.l., Linfa ShPK, Lis S.r.l., Idea 75 S.r.l., DecHit S.p.A., Codd&Date S.r.l.
- **IA Generativa:** sistemi di IA capaci di generare contenuti originali (testi, immagini, codice, audio, video).
- **Modelli di intelligenza artificiale**: i modelli definiti dall'articolo 3, punto 63), del regolamento (UE) 2024/1689 (modelli di IA per finalità generali), ossia modelli che, anche se addestrati con grandi quantità di dati mediante autosupervisione su larga scala, presentano una generalità significativa, sono in grado di svolgere con competenza un'ampia gamma di compiti distinti e possono essere integrati in una varietà di sistemi o applicazioni a valle.
- **Sistema ad Alto Rischio:** sistema IA che rientra nella classificazione dell'AI Act per il suo potenziale impatto su diritti fondamentali, sicurezza o processi critici.
- **Sistema di Intelligenza Artificiale:** sistema definito dall'art. 3, punto 1, del Regolamento (UE) 2024/1689, ossia un sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dagli input ricevuti come generare output – quali previsioni, contenuti, raccomandazioni o decisioni – in grado di influenzare ambienti fisici o virtuali.
- **Supervisione Umana:** intervento qualificato di operatori per validare, correggere o intervenire sulle decisioni automatizzate.
- **Workflow agentico (Workflow AI):** processo o sottoprocesso aziendale assistito o automatizzato mediante strumenti IA, eseguito in tutto o in parte da Agenti IA con supervisione umana.

# 4 Riferimenti normativi

La presente Policy è stata redatta in conformità alle seguenti fonti normative:

- **Regolamento (UE) 2024/1689** (AI Act), come successivamente modificato;
- **Linee guida della Commissione europea** sugli obblighi di trasparenza per i sistemi di IA ex art. 50 AI Act (20 luglio 2026);
- **Code of Practice on Transparency of AI-Generated Content** (Commissione europea, 10 giugno 2026);
- **Legge 23 settembre 2025, n. 132** - Disposizioni in materia di intelligenza artificiale;
- **Regolamento (UE) 2016/679** (GDPR);

- **D.Lgs. 196/2003** - Codice Privacy;
- **D.lgs 10 agosto 2018, n. 101** - Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali;
- **D.Lgs. 81/2008** - Testo Unico sulla Sicurezza;
- **Statuto dei Lavoratori** (L. 300/1970), art. 4;
- **Linee Guida** per l'implementazione dell'IA nel mondo del lavoro (Decreto Ministeriale 17 dicembre 2025, n. 180);
- **Carta dei Diritti Fondamentali dell'UE;**
- **ISO/IEC 42001** - Sistemi di gestione per l'intelligenza artificiale;
- **ISO/IEC 27001** - Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni.

# 5 Principi generali

Il Gruppo Links si impegna a utilizzare l'IA secondo i seguenti principi fondamentali:

- **Accountability**: ogni utilizzo di IA ha un Responsabile identificabile che risponde delle decisioni e degli impatti.
- **Centralità della persona (Human-Centric AI)**: l'IA è uno strumento a supporto dell'attività umana, non un sostituto del giudizio professionale.
- **Equità e non discriminazione**: i sistemi IA non devono generare o amplificare discriminazioni basate su genere, età, etnia, disabilità, orientamento politico o altre caratteristiche protette.
- **Privacy by design**: la protezione dei dati personali è integrata fin dalla progettazione dei sistemi IA.
- **Sicurezza e affidabilità**: i sistemi IA devono operare in modo sicuro, con adeguate misure di Cybersecurity lungo tutto il ciclo di vita.
- **Sostenibilità**: l'adozione dell'IA deve contribuire al miglioramento delle condizioni di lavoro e alla crescita sostenibile dell'organizzazione.
- **Trasparenza e spiegabilità**: i lavoratori devono essere informati quando l'IA viene utilizzata nei processi che li riguardano e hanno diritto a comprenderne la logica decisionale.

# 6 Governance dell'IA

Al fine di garantire un utilizzo della IA che sia etico e che abbia come punto di riferimento centrale la persona, Links e le aziende del Gruppo nominano delle figure di riferimento di seguito descritte.

## 6.1 Responsabile IA (Chief Artificial Intelligence Officer - CAIO) e Comitato AI

Il Gruppo Links nomina un **Responsabile IA** e istituisce un **Comitato AI**, assegnando loro i poteri e le funzioni di seguito descritti. Il Responsabile IA (CAIO) ha i seguenti compiti:

- Compliance normativa e documentale
- Governance tecnica dei Sistemi IA
- Relazioni industriali e tutela dei lavoratori
- Formazione e sviluppo competenze
- Gestione Fornitori e contratti IA
- Supporto per il Risk Management e Incident Response
- Reporting e comunicazione istituzionale
- Coordinamento con altre funzioni aziendali
- Interfaccia con le autorità competenti (ACN, AgID, Garante Privacy).

Per l'espletamento efficace delle funzioni assegnate, il CAIO è dotato dei seguenti poteri e risorse:

- **Autonomia funzionale**: il CAIO opera con autonomia funzionale nello svolgimento dei propri compiti, riferendo alla Direzione aziendale e raccordandosi con il Comitato AI per le decisioni di maggiore rilevanza;
- **Accesso alle informazioni**: il CAIO ha accesso alla documentazione aziendale rilevante per le proprie funzioni, inclusi contratti, licenze software, configurazioni tecniche e dati di utilizzo dei sistemi IA;
- **Sospensione cautelativa**: in caso di non conformità grave o di rischio imminente, il CAIO può disporre la sospensione cautelativa dell'utilizzo di un sistema IA, dandone comunicazione contestuale alla Direzione e al Comitato AI, che ne valuta la conferma;
- **Supporto organizzativo**: il CAIO può avvalersi del supporto delle funzioni aziendali (CISO, ITS, IM, HRO, LEG, Amministrazione), previo coordinamento con i rispettivi Responsabili.

Il **Comitato AI** multidisciplinare è composto da:

- Responsabile IA (CAIO);
- Responsabile Risorse Umane (HRL);
- Responsabile Security (CISO);
- Head of Competence Center IT Services & Digital Security (HCC ITS);
- Referente delle strutture produttive (Head of Competence Center);
- Referente delle strutture commerciali (Industry Lead o Client Lead);

- Rappresentanti dei lavoratori;
- Ufficio legale (LEG) e procurement (PRO).

Il Comitato si riunisce almeno **trimestralmente** e valuta e indirizza i seguenti ambiti, a supporto e conferma dell'indirizzo aziendale:

- Aggiornamento della Policy e del Registro dei Sistemi IA;
- Valutazione etica dei nuovi progetti IA e analisi di impatto sui lavoratori;
- Valutazione delle strategie e attivazione di iniziative per soluzioni IA;
- Gestione delle licenze IA e correlati adeguamenti organizzativi e sistemistici;
- Contrattualizzazione e valutazione dei Fornitori di soluzioni IA;
- Formazione e sviluppo competenze;
- Gestione di segnalazioni e controversie.

Il Comitato assume inoltre **poteri decisionali**: in **supplenza** del CAIO, in caso di sua assenza, impedimento o vacanza della carica; a **supporto** del CAIO, quando una decisione ne ecceda i poteri o presenti particolare complessità etica, giuridica o contrattuale; a **conferma** delle sospensioni cautelative disposte dal CAIO.

Le decisioni del Comitato sono documentate e comunicate alla Direzione; le modalità operative di funzionamento sono definite nelle disposizioni attuative della presente Policy.

Il CAIO e il Comitato AI possono delegare per iscritto specifiche funzioni operative a propri **delegati**, individuati tra i membri del Comitato o tra i Responsabili di Funzione o altre figure identificate.

## 6.2 Registro dei Sistemi IA

Links predispone e mantiene aggiornato un **Registro** indicante l'elenco di tutti i sistemi IA utilizzati, contenente almeno le seguenti informazioni:

- Denominazione e descrizione del Sistema IA;
- Classificazione del rischio (AI Act);
- Finalità utilizzo;
- Tipologia di dati trattati;
- Responsabile del sistema;
- Misure di mitigazione dei rischi;
- Autorizzazione utilizzo;
- GDPR Compliance;
- DPA.

Tutti i Sistemi IA, prima del loro utilizzo in azienda e conseguente annotazione nel Registro, **devono essere approvati dal CAIO**, previa Analisi dei Rischi e/o DPIA.

Il Gruppo Links definisce altresì le procedure per **richiedere integrazioni o eventuali deroghe al CAIO** per strumenti, finalità, tipologie di dati trattati e misure di mitigazione dei rischi non incluse nel registro e/o non autorizzate.

Il Registro è accessibile a tutta la popolazione di Links e alle Aziende del Gruppo, al CISO, al DPO, al Comitato AI e, nelle parti pertinenti, ai rappresentanti dei lavoratori nonché gli Enti preposti al controllo, esempio il TUV.

# 7 Ambiti di utilizzo autorizzati

Il Gruppo Links utilizza sistemi di IA nei seguenti ambiti, nel rispetto dei principi e delle regole operative definiti nella presente Policy e altra documentazione aziendale, nonché quanto pertinente ai **Sistemi di Gestione ISO/IEC** adottati.

**A. Sviluppo Software**

- Code generation e debugging (con revisione umana);
- Build/Setup/Configuration/Test Automation;
- Vulnerability Assessment e Penetration Test;
- Documentazione tecnica, funzionale. Design UX/UI.

**B. Supporto operativo e documentale**

- Riformulazione e correzione di testi non sensibili;
- Traduzione di documenti pubblici;
- Generazione di bozze di procedure interne;
- Sintesi di documentazione tecnica pubblica;
- Elaborazioni di relazioni, report, analisi utili per l'espletamento delle proprie mansioni lavorative.

**C. Supporto alla comunicazione**

- Assistenza nella redazione di comunicazioni esterne standard;
- Generazione di contenuti per marketing (previa verifica umana);
- Ottimizzazione di newsletter e materiali promozionali.

**D. Analisi dati e Business Intelligence**

- Analisi predittive su dati aggregati e anonimizzati;
- Ottimizzazione di processi produttivi;
- Supporto decisionale strategico (con supervisione umana obbligatoria).

**E. Formazione del personale**

- Piattaforme di e-learning adattivo;
- Generazione di materiali formativi;
- Simulazioni e training.

**F. Automazione processi interni**

- Classificazione e smistamento automatico di ticket, richieste e segnalazioni;
- Automazione di flussi di Workflow di back-Office (con supervisione umana obbligatoria);
- Monitoraggio operativo e Alerting su anomalie (SLA, KPI, scostamenti);
- Generazione automatica di verbali e minute da riunioni;
- Assistenza nella compilazione di moduli, Timesheet e reportistica ricorrente;
- Categorizzazione e tagging automatico di asset documentali e knowledge base;
- Orchestrazione di Task ripetitivi cross-sistema (con supervisione umana obbligatoria).

# 8 Rapporti con i Clienti

## 8.1 Principi generali

La presente Policy definisce i **requisiti minimi** del Gruppo Links: nei progetti per i Clienti prevalgono i requisiti **più stringenti** previsti dal contratto o dalla policy AI del Cliente. I **divieti assoluti** e gli **obblighi di legge** costituiscono in ogni caso un livello minimo **inderogabile**.

## 8.2 Comunicazione e policy AI del Cliente

Links **informa il Cliente** dell'utilizzo di strumenti e processi assistiti o automatizzati con IA:

- **informativa scritta** in fase di offerta o avvio progetto, aggiornata in caso di variazioni rilevanti;
- richieste e restrizioni del Cliente **recepite** nelle modalità operative e, ove necessario, formalizzate contrattualmente;
- ove esista una **policy AI del Cliente**, il **Project Lead (PL)** e il **Responsabile di struttura** ne verificano la compatibilità e ne recepiscono i vincoli;
- eventuali **conflitti** sono segnalati al **CAIO** e al **Comitato AI**.

## 8.3 Strumenti, ambienti e registri

Alle combinazioni di strumenti, ambienti e registri di Links e del Cliente si applicano i seguenti criteri:

In ogni caso, anche in ambienti e con regole del Cliente:

- i **divieti assoluti** e gli **obblighi di legge** si applicano **sempre**;
- le disposizioni Links **più restrittive** si applicano ove tecnicamente e contrattualmente possibile; le impossibilità sono segnalate dal Project Lead (PL) al CAIO;
- in caso di sovrapposizione prevale la **disposizione più restrittiva**.

| Strumento | Ambiente | Regole applicabili |
|---|---|---|
| Links | Links | **Policy AI** e **Registro dei Sistemi IA** di Links (caso standard). |
| Links | Cliente | Policy AI e Registro dei Sistemi IA di Links **e** autorizzazione del Cliente, secondo la policy AI e il registro del Cliente, ove esistenti. |
| Cliente | Cliente | Policy AI e registro del Cliente; restano fermi i divieti assoluti della presente Policy. |
| Cliente | Links | **Richiesta approvazione CAIO di Links** e censimento nel Registro dei Sistemi IA di Links, nel rispetto delle condizioni del Cliente. |

## 8.4 Ruolo di Links ai sensi dell'AI Act

Nei progetti per i Clienti, Links opera esclusivamente quale **deployer** e **non assume il ruolo di provider** ai sensi del Regolamento (UE) 2024/1689: le soluzioni sono di titolarità del Cliente, che eroga il servizio, anche quando Links ne realizza l'integrazione. Richiedono un **approfondimento preventivo** con CAIO, Comitato AI e Ufficio legale i seguenti **casi di attenzione** per l'eventuale qualificazione come **provider**:

- immissione sul mercato di un sistema IA con nome o marchio Links;
- commercializzazione di un prodotto o soluzione IA propria;
- modifica sostanziale di un sistema IA o della sua finalità;
- fine-tuning o specializzazione rilevante di un modello per finalità generali;
- modelli di terze parti esposti tramite interfacce o servizi a marchio Links.

## 8.5 Dati, codice e documentazione del Cliente

L'accesso e il trattamento di dati, codice e documentazione del Cliente rientrano nella normale esecuzione del progetto e sono disciplinati da **contratto**, **accordi sul trattamento dei dati** e **GDPR**. Il trattamento mediante strumenti IA è consentito nei limiti della presente Policy, della policy AI del Cliente ove esistente, e della normativa vigente.

- Eventuali **vincoli specifici** (es. data residency UE, trattamento di materiale confidenziale con inferenza locale o specifici modelli, esclusione di specifici dati, codici e materiali) sono espressi dal Cliente e **concordati in fase di offerta, contratto o avvio**, poiché incidono su soluzioni, tempi e costi.

## 8.6 Vincoli sopravvenuti

I vincoli introdotti o modificati dal Cliente in corso d'opera (es. adozione o revisione della propria policy AI) sono gestiti come **variazione di progetto**: Project Lead (PL) e Responsabile di struttura ne valutano gli impatti e concordano un **piano di adeguamento** formalizzato. Nelle more restano validi gli **accordi previgenti**, salvo richiesta di **sospensione cautelativa** nell'utilizzo degli strumenti AI da parte del CAIO o del Cliente; restano fermi divieti assoluti e obblighi di legge. I conflitti sono rimessi al CAIO e al Comitato AI.

# 9 Condizioni d'utilizzo ed utilizzi vietati o ad alto rischio

## 9.1 Condizioni generali per tutti gli ambiti di utilizzo

Tutti i Sistemi AI autorizzati, indipendentemente dall'ambito di utilizzo e dalla tipologia di dati trattati, richiedono:

- Supervisione umana obbligatoria;
- Verifica della qualità degli output;
- Nessun trattamento di dati sensibili senza garanzie adeguate.

## 9.2 Divieti assoluti

È **vietato** utilizzare Sistemi di IA per:

- **Decisioni automatizzate** che incidono significativamente sui **diritti dei lavoratori** (assunzioni, licenziamenti, promozioni) **senza supervisione umana qualificata**;
- **Sorveglianza emotiva o biometrica dei lavoratori** (salvo casi previsti dalla legge);
- Manipolazione psicologica o comportamentale;

- **Social Scoring** dei **dipendenti**;
- Riconoscimento facciale in tempo reale in spazi accessibili al pubblico (salvo eccezioni di legge);
- Navigazione ed esplorazione automatizzata portali e contenuti privati di Links o dei clienti tramite l'utilizzo di **Browser AI** o **Estensioni AI**, quali a titolo esemplificativo e non esaustivo browser OpenAI Atlas, Arc Max, Perplexity Comet e/o estensione Claude per browser.

## 9.3 Utilizzi ad alto rischio (richiedono autorizzazione del CAIO)

- Selezione e valutazione del personale;
- Sistemi di monitoraggio delle performance;
- Sistemi di allocazione automatica di turni o mansioni;
- Analisi di dati personali per finalità organizzative.

## 9.4 Informazioni che NON devono essere caricate su IA generativa pubblica

È **severamente vietato** inserire su strumenti di IA generativa non autorizzati (es. versioni gratuite di ChatGPT, Gemini, ecc.) i seguenti dati e informazioni:

- **Dati personali** di colleghi, clienti o terzi;
- **Dati sensibili** ai sensi dell'art. 9 GDPR;
- **Informazioni commerciali riservate** (listini, preventivi, strategie);
- **Proprietà intellettuale** (codice sorgente, progetti, brevetti di proprietà delle società del Gruppo Links, documentazione dei Clienti, codice sorgente completo del Cliente);
- **Contratti, NDA e documenti legali riservati**;
- **Credenziali di accesso o informazioni di sicurezza**;
- Codici seriali, licenze, API Token.

# 10 Regole operative generiche per l'utilizzo dell'IA

## 10.1 Utilizzo di IA Generativa

Links Group **autorizza** esclusivamente l'utilizzo degli strumenti presenti nel Registro IA **con licenze aziendali gestite centralmente** e/o **licenze personali associate a indirizzi E-mail aziendali**.

Ogni strumento e/o piattaforma che utilizzi l'IA deve essere censito all'interno di apposito **Registro** e **singolarmente approvato dal CAIO** o da un **delegato** del CAIO.

L'utilizzo delle licenze personali associate a indirizzi E-mail aziendali è consentito solo con le seguenti condizioni:

- lo strumento AI è pre-autorizzato nel Registro Sistemi IA per la finalità di utilizzo e per la tipologia di dati trattati;
- tutte le misure di mitigazione dei rischi di sicurezza sono state attivate;
- notifica di adozione dello strumento IA al CAIO tramite procedura dedicata.

È altresì **vietato il caricamento di qualunque tipologia di dati** sopra citati nei **Sistemi IA** senza registrazione e/o con **licenze personali associate a indirizzi E-mail personali**.

## 10.2 Adozione degli strumenti IA nei progetti e nelle attività

L'**autorizzazione** di uno strumento nel **Registro dei Sistemi IA** non ne comporta l'**adozione automatica** nei progetti e nelle attività aziendali. L'impiego di strumenti e di **processi assistiti o automatizzati con strumenti IA** in uno specifico progetto o attività è valutato e autorizzato dal **Project Lead (PL)** e dal **Responsabile di struttura**, che verificano almeno:

- i **vincoli contrattuali** e la **policy AI del Cliente**, ove esistenti (sezione "Rapporti con i Clienti");
- la **tipologia di dati trattati** e le misure previste dal Registro;
- gli impatti su **soluzioni, tempi e costi**;
- **qualsivoglia ulteriore necessità** rilevante per il contesto specifico.

Gli esiti della valutazione sono **tracciati** nella documentazione di progetto o di struttura e **comunicati, insieme a eventuali deroghe** rispetto alla presente Policy o al Registro, **al CAIO e al Comitato AI** secondo le disposizioni attuative della presente Policy.

# 10.3 Configurazione obbligatoria

Per **ogni strumento autorizzato l'utilizzatore deve**:

- **Disattivare** l'opzione "Usa i miei dati per migliorare il modello" (o analoghe) e/o attivare le modalità "Privacy" che vietano l'utilizzo o il mantenimento di dati per finalità non coerenti con l'attività (qualora possibile);
- Utilizzare **account aziendali** con gestione centralizzata o notificare al CAIO l'utilizzo con account aziendale e licenza personale tramite apposita procedura;
- Verificare che i dati **non siano trasferiti extra-UE** (o con adeguate garanzie). Il CAIO può eventualmente rendere disponibili adeguate verifiche all'interno del registro Sistemi IA pre-autorizzati;
- Verificare **che le finalità d'utilizzo e la tipologia di dati da trattare siano pre-autorizzate** nel registro Sistemi AI;
- Disattivare, qualora possibile, o astenersi dall'interagire con qualsiasi meccanismo di valutazione o segnalazione integrato nell'interfaccia dello strumento IA (es. icone di gradimento, pulsanti di feedback, segnalazione errori); tali interazioni possono rendere disponibili i contenuti delle conversazioni al fornitore per finalità di revisione e addestramento, indipendentemente da quanto configurato rispetto all'utilizzo e mantenimento dati. È possibile richiedere al CAIO autorizzazioni specifiche in deroga o integrazione al registro.

## 10.3.1 Procedura operativa

1. **Prima di utilizzare l'IA:**
    - Verificare che lo strumento sia nella lista autorizzata;
    - Assicurarsi di non inserire dati riservati o personali;
    - Assicurarsi di aver attivato o configurato le misure minime di mitigazione dei rischi di sicurezza (indicati all'interno del registro Sistemi IA);
    - Anonimizzare qualsiasi riferimento identificativo.
2. **Durante l'utilizzo:**
    - Formulare prompt chiari evitando dettagli sensibili (dati personali dell'utente, dati del Cliente, dati aziendali del Gruppo Links);
    - Non fare affidamento completo sugli output ma effettuare sempre una scrupolosa verifica;
    - Documentare l'uso per le attività critiche.
    - Astenersi dall'utilizzare qualsiasi funzionalità di valutazione o segnalazione feedback dello strumento IA (es. icone di gradimento, pulsanti di feedback, segnalazione errori al fornitore).
3. **Dopo l'utilizzo:**

- Verificare accuratezza e conformità dell'output;
- Correggere errori o "allucinazioni";
- Cancellare conversazioni contenenti dati sensibili (se previsto dallo strumento);
- Indicare, quando appropriato, che il contenuto è stato generato con il supporto di Strumenti IA. Si applica la classificazione ed etichettatura dei contenuti definita dalla presente Policy.
- Memorizzare ed archiviare il contenuto su sistemi aziendali (es. OneDrive, Git, ...) se lo strumento AI è utilizzato tramite interfaccia web e servizi remoti e Cloud.

## 10.4 Supervisione umana obbligatoria

Ogni decisione rilevante supportata da IA deve essere:

- **Validata** da un operatore competente;
- **Tracciata** con indicazione del responsabile;
- **Contestabile** dal soggetto interessato.

La **supervisione umana** è altresì **obbligatoria per lo Sviluppo Software** e per ogni "**prodotto**" destinato ai **Clienti** del **Gruppo Links**.

## 10.5 Documentazione e tracciabilità

In caso di utilizzo **sistemi IA ad alto rischio**, il Gruppo Links mantiene:

- Log delle decisioni automatizzate (qualora utilizzate);
- Documentazione tecnica del sistema;
- Valutazioni di impatto (DPIA quando necessaria);
- Report di Audit periodici.

Links definisce le modalità e responsabilità di archiviazione della documentazione su indicata e garantisce il censimento all'interno di apposito **Registro** con utilizzo **singolarmente approvato dal CAIO** o da un **delegato** del CAIO.

## 10.6 Classificazione ed etichettatura dei contenuti generati con IA

Il Gruppo Links classifica i contenuti prodotti con l'ausilio dell'IA nei seguenti **livelli**, in coerenza con gli obblighi di trasparenza dell'art. 50 AI Act, con le relative Linee guida della Commissione europea e con la L. 132/2025.

Le modalità e le condizioni di classificazione ed etichettatura sono definite nelle disposizioni attuative della presente Policy.

## 10.7 Workflow agentici

Il Gruppo Links promuove la **trasformazione dei processi aziendali** mediante l'introduzione progressiva di **Workflow agentici**, di **Agenti IA** a supporto delle attività e delle relative **Checklist** operative (es. produzione documentale, analisi funzionali, sviluppo codice, generazione ed esecuzione di test, estrazione di conoscenza da codebase).

I Workflow agentici e le relative Checklist sono approvati dal **CAIO** d'intesa con il **Comitato AI** e costituiscono il **riferimento vincolante** per le attività cui si applicano; gli scostamenti sono gestiti come deroghe notificate al CAIO. Sono garantite la **supervisione umana**, la **documentazione** ai fini di auditing e trasparenza, la **tracciabilità** e, per quanto tecnicamente possibile, la **replicabilità** delle decisioni assunte con il supporto dell'IA. I requisiti di dettaglio sono definiti nelle **disposizioni attuative** della presente Policy.

## 10.8 Telemetria e tracciature (Logging)

Gli **strumenti IA adottati aziendalmente**, i **Workflow agentici** e gli **Agenti IA** sono configurati, ove tecnicamente supportato, per la **raccolta di telemetria e tracciature di log**, comprensive di metriche di utilizzo e consumo (sessioni, Token, costi per modello), eventi di interazione (prompt e risposte, messaggi tra Agenti e tra Agente e utente), utilizzo di Tool e Componenti di integrazione IA ed esiti delle azioni.

La raccolta è effettuata per le seguenti **finalità**:

- adempimento degli obblighi di **registrazione, tracciabilità e supervisione** (artt. 12 e 26 del Regolamento (UE) 2024/1689; L. 132/2025; ISO/IEC 42001 e 27001);
- **sicurezza, auditing e Incident Response**;
- analisi delle **modalità di utilizzo** degli strumenti IA, a supporto del miglioramento continuo di processi, Workflow e Checklist;
- **monitoraggio, valutazione e ottimizzazione dei costi**, nonché corretto dimensionamento di licenze e capacità;
- valutazione comparativa di **modelli, strumenti e Fornitori**, a supporto delle decisioni di adozione e di evoluzione tecnologica.

La raccolta avviene nel rispetto del **GDPR** e dell'**art. 4 della L. 300/1970**: i lavoratori ricevono **preventiva e adeguata informativa** sulle modalità d'uso degli strumenti e di effettuazione dei controlli (art. 4, comma 3, L. 300/1970; artt. 12 e 13 GDPR); i dati raccolti **non sono utilizzati per il monitoraggio o la valutazione della prestazione lavorativa**; le analisi sono condotte, ove possibile, su dati **aggregati o pseudonimizzati**; gli accessi sono limitati, profilati e tracciati; i tempi di conservazione sono minimizzati; ove richiesto è condotta una **DPIA** con il coinvolgimento del DPO. I requisiti di dettaglio sono definiti nelle **disposizioni attuative** della presente Policy.

# 11 Trattamento dei dati e Privacy

## 11.1 Tipologie di dati trattati con l'uso dell'IA

Il Gruppo Links categorizza, ai fini della gestione dei dati trattati con gli strumenti AI, le seguenti tipologie di dati:

A. **Dati personali, confidenziali e sensibili** (trattamento non consentito);
   - Dati identificativi, di contatto e professionali;
   - Dati contrattuali e retributivi;
   - Dati di navigazione, log applicativi e localizzazione;
   - Credenziali e dati di autenticazione;
   - Categorie particolari (art. 9: biometrici, salute, origine etnica, opinioni politiche, appartenenza sindacale, genetici, orientamento sessuale);
   - Dati relativi a condanne penali e reati (art. 10);
   - Dati inferiti e derivati riconducibili a persone fisiche (scoring, profili comportamentali, sentiment, classificazioni algoritmiche);
   - Dati confidenziali identificati in DPIA.

B. **Dati di codice, progetto e infrastruttura**
   - Codice sorgente proprietario, librerie interne, configurazioni;
   - Codice di terze parti e dipendenze Open Source;
   - Prompt, template e system instruction per LLM;
   - Output IA integrati nel Deliverable (codice, test, documentazione);
   - Vulnerability Report e Finding di sicurezza;
   - Documentazione di offerta, capitolati, specifiche funzionali e tecniche;
   - Piani di progetto, Effort, Milestone, SAL, verbali;
   - Log di sistema e di sicurezza (SIEM, WAF, IDS) ad esclusione di quelli che includono dati personali, confidenziali e sensibili;
   - Metriche di performance e telemetria (APM, Observability);
   - Configurazioni infrastrutturali (IaC, Manifest K8s, Pipeline CI/CD);
   - Asset Inventory (CMDB, Licenze, Endpoint).

C. **Dati di comunicazione, mercato e intelligence**
   - Contenuti editoriali e promozionali (Newsletter, Blog, Social);

- Dati di Engagement e Analytics (aperture, Click, conversioni);
- Liste di contatti e segmentazione audience;
- Brand Asset e materiali grafici;
- Informazioni pubbliche su competitor, trend, bandi;
- Benchmark settoriale e analisi di mercato;
- Corrispondenza commerciale e progettuale.

D. **Dati di knowledge management e formazione**

- Knowledge Base interna e FAQ;
- Materiali didattici e percorsi e-Learning;
- Assessment, quiz e risultati di valutazione;
- Registrazioni di sessioni formative (audio/video);
- Procedure interne, Policy e regolamenti aziendali;

E. **Dati contrattuali e legali** (trattamento consentito solo nel rispetto di accordi e termini di riservatezza e protezione della proprietà intellettuale e con applicazione di misure di mitigazione dei rischi riportate nel Registro ovvero anonimizzazione dei dati):

- Testi contrattuali (Clienti, Fornitori, Partner, NDA);
- Clausole e condizioni di licenza Software;
- Documentazione di gara e appalto;
- Pareri legali e documentazione di compliance.

F. **Dati sintetici, di addestramento e della supply chain AI**

- Dataset sintetici generati per test e sviluppo;
- Dati anonimizzati o pseudonimizzati per fine-tuning;
- Benchmark e Golden Dataset per validazione;
- Annotazioni e Labeling umano;
- Modelli pre-addestrati e Training Data Summary (obbligo gpai);
- API e servizi IA esterni (Provider, SLA, Data Residency);
- Risultati di Audit e certificazioni dei Fornitori IA.

## 11.2 Principi relativi alla Privacy e al GDPR nell'uso dell'IA

Tutti i trattamenti di dati personali tramite IA devono rispettare:

- **Liceità, correttezza, trasparenza** (art. 5 GDPR);
- **Limitazione delle finalità;**
- **Minimizzazione dei dati;**
- **Esattezza;**
- **Limitazione della conservazione;**
- **Integrità e riservatezza.**

## 11.3 Informativa agli interessati

Le società del **Gruppo Links informano i lavoratori e gli interessati** quando **sono utilizzati sistemi di IA che trattano i loro dati**, specificando:

- Finalità e basi giuridiche;
- Logica del trattamento automatizzato;
- Conseguenze previste;
- Diritti degli interessati (accesso, rettifica, opposizione, ecc.).

## 11.4 Diritto di opposizione (Art. 22 GDPR)

Nessun **lavoratore** può essere sottoposto a **decisioni** basate **unicamente** su trattamenti automatizzati con effetti significativi, senza:

- Intervento umano qualificato;
- Possibilità di esprimere la propria opinione;
- Diritto di contestare la decisione.

## 11.5 Data Protection Impact Assessment (DPIA)

Per sistemi ad **alto rischio**, Links conduce una **DPIA** prima dell'implementazione, coinvolgendo il DPO e consultando, se necessario, il Garante Privacy.

## 11.6 Anonimizzazione e pseudonimizzazione

Quando possibile, le società del Gruppo Links utilizzano dati anonimizzati o pseudonimizzati per addestrare o alimentare Sistemi IA, seguendo le migliori pratiche internazionali.

# 12 Sicurezza e Cybersecurity

## 12.1 Sicurezza dei sistemi IA

Il Gruppo Links implementa misure tecniche e organizzative per garantire:

- **Integrità dei dati** utilizzati per l'addestramento;
- **Controllo degli accessi** (Autenticazione, autorizzazione);
- **Protezione contro attacchi** (Adversarial Attacks, Data Poisoning, Direct Prompt Injection);
- **Resilienza operativa** (Backup, Disaster Recovery).

Nel Registro dei Sistemi IA sono altresì riportate le misure minime di mitigazione dei rischi di sicurezza per ogni specifico strumento.

## 12.2 Gestione delle vulnerabilità

- Aggiornamenti regolari dei sistemi IA;
- Vulnerability Assessment periodici;
- Patch Management tempestivo;
- Incident Response Plan specifico per IA, in collaborazione con l'Incident Manager.

## 12.3 Supply Chain Security

I Fornitori di Soluzioni IA devono:

- Garantire **conformità** all'**AI Act**, alle normative italiane e al **GDPR**;
- Fornire **documentazione tecnica trasparente**;
- Sottoporsi ad **Audit** di **Sicurezza**;
- Notificare tempestivamente eventuali **Data Breach**.

# 13 Diritti e tutele dei lavoratori

## 13.1 Diritto all'informazione

Ogni **lavoratore ha diritto di essere informato**:

- Quando l'IA viene utilizzata in processi che lo riguardano;

- Sulla logica e i criteri decisionali del sistema;
- Sui dati personali trattati e sulle finalità.

## 13.2 Diritto alla spiegazione

I lavoratori possono **richiedere spiegazioni** comprensibili su:

- Come funziona il Sistema IA utilizzato;
- Quali dati sono stati considerati;
- Come è stata raggiunta una determinata decisione.

## 13.3 Diritto di contestazione

Ogni lavoratore può:

- **Contestare decisioni automatizzate** che lo riguardano;
- Richiedere una **revisione umana**;
- Presentare **osservazioni** e **reclami**, anche attraverso la piattaforma di **Whistleblowing** di Links.

## 13.4 Canali di segnalazione

Links garantisce **canali riservati** per segnalare:

- Presunte violazioni di questa Policy;
- Utilizzi impropri dell'IA;
- Discriminazioni o Bias algoritmici;
- Violazioni dei diritti fondamentali.

## 13.5 Modalità di segnalazione

- E-mail **dedicata**: etica.ia@linksmt.it;
- Piattaforma **Whistleblowing** aziendale (ai sensi del D.Lgs. 24/2023);
- **Comitato AI**.

## 13.6 Garanzie

- Riservatezza assoluta dell'identità del segnalante;

- Protezione da ritorsioni;
- Gestione tempestiva delle segnalazioni (risposta entro 15 giorni lavorativi).

## 13.7 Tutela dal controllo a distanza (Art. 4 Statuto dei Lavoratori)

L'utilizzo di sistemi IA per il controllo dell'attività lavorativa è consentito solo:

- Previo accordo con le rappresentanze sindacali o autorizzazione dell'Ispettorato del Lavoro;
- Con informativa trasparente ai lavoratori;
- Nel rispetto della finalità dichiarata (sicurezza, organizzazione, non controllo).

# 14 Formazione e sensibilizzazione

## 14.1 Programma formativo obbligatorio

Il Gruppo Links garantisce a tutti i dipendenti interventi di formazione e Awareness, come di seguito definito:

- **Formazione di base sull'IA** (entro 3 mesi dall'assunzione):
  - Cos'è l'IA e come funziona;
  - Rischi e opportunità;
  - Principi etici e normativi;
  - Contenuti di questa Policy.
- **Formazione specifica** per chi utilizza strumenti IA:
  - Uso corretto e sicuro degli strumenti;
  - Riconoscimento di Bias ed errori;
  - Anonimizzazione e protezione dei dati;
  - Gestione di situazioni critiche.
- **Formazione avanzata** per responsabili e decisori:
  - Governance dell'IA;
  - Valutazione dei rischi;
  - Compliance normativa;
  - Leadership etica.

## 14.2 Aggiornamento continuo

La formazione viene aggiornata **almeno annualmente** per riflettere:

- Evoluzioni tecnologiche;
- Modifiche normative;
- Nuovi casi d'uso aziendali;
- Lesson Learned da Audit e segnalazioni.

# 15 Monitoraggio, Audit e revisione

## 15.1 Monitoraggio continuo

Il CAIO monitora costantemente:

- Utilizzo dei Sistemi IA autorizzati;
- L'impiego e la distribuzione delle Licenze aziendali;
- Conformità alle procedure operative;
- Indicatori di performance e rischio;
- Segnalazioni e reclami.

## 15.2 Audit periodici

Il Gruppo Links conduce audit **almeno semestrali** su:

- Sistemi IA ad alto rischio (ogni 6 mesi);
- Conformità alla Policy e alle normative;
- Efficacia delle misure di sicurezza;
- Impatto sui lavoratori e sui processi.

Gli audit possono essere:

- **Interni** (condotti dal Comitato AI, Auditor qualificati ISO/IEC 42001);
- **Esterni** (da Enti certificatori indipendenti per sistemi critici).

## 15.3 Valutazione dei Bias

Almeno **annualmente**, il Gruppo Links valuta:

- Presenza di Bias nei sistemi IA;

- Impatto su gruppi protetti o vulnerabili;
- Efficacia delle misure di mitigazione.

## 15.4 Revisione della Policy

Questa Policy viene revisionata con cadenza **annuale** e in caso di modifiche normative rilevanti, nonché a seguito di Incidenti significativi.

# 16 Gestione delle violazioni

## 16.1 Classificazione delle violazioni

**Violazioni minori**

- Utilizzo non autorizzato di strumenti IA per attività non critiche;
- Mancata anonimizzazione di dati in contesti a basso rischio;
- Ritardo nella documentazione o nelle comunicazioni.

**Violazioni gravi**

- Inserimento di dati personali o riservati in IA pubblica;
- Utilizzo di IA per decisioni automatizzate senza supervisione;
- Mancata informativa ai lavoratori interessati;
- Disattivazione di misure di sicurezza;
- Utilizzo di funzionalità di Feedback integrato negli strumenti IA (Thumbs Up/Down, Rating, Flag o simili).

**Violazioni gravissime**

- Utilizzi vietati (sorveglianza biometrica non autorizzata, social scoring, ecc.);
- Discriminazione intenzionale tramite IA;
- Violazione massiva di dati personali;
- Occultamento di violazioni.

## 16.2 Sanzioni disciplinari

In base alla gravità e alla reiterazione, le violazioni possono comportare:

- **Richiamo verbale** e **formazione correttiva**;
- **Richiamo scritto**;

- **Sospensione** dall'**utilizzo di strumenti IA**;
- **Sanzioni disciplinari ai sensi del CCNL**;
- Nei **casi più gravi, licenziamento per giusta causa**.

## 16.3 Procedimento

- Accertamento dei fatti da parte del CAIO;
- Audizione del soggetto interessato;
- Decisione motivata **entro 30 giorni**;
- Possibilità di **ricorso al Comitato AI**.

## 16.4 Obbligo di notifica

Le violazioni che comportano **rischi per i diritti e le libertà delle persone sono notificate**:

- Al CAIO e al CISO (immediatamente);
- Al DPO (immediatamente);
- Al Garante Privacy (entro 72 ore, se applicabile);
- Alle autorità competenti (ACN, AgID) nei casi previsti dall'AI Act e altre normative vigenti.

# 17 Disposizioni finali

## 17.1 Clausola di adeguamento normativo

In caso di modifiche alla normativa europea o nazionale, il Gruppo Links si impegna ad adeguare tempestivamente la presente Policy, anche in via interpretativa, per garantire piena conformità.

## 17.2 Disposizioni attuative

Le **modalità operative di attuazione** della presente Policy (procedure, flussi di notifica e comunicazione, modelli e strumenti) sono definite dal **CAIO**, d'intesa con il **Comitato AI**, e **comunicate successivamente** al personale attraverso i canali aziendali. Tali disposizioni integrano la presente Policy senza modificarne i principi.




Links group | Links LOS Nexus idee75 codd&date