REGOLAMENTO PER UN USO CORRETTO E CONSAPEVOLE DELL'INTELLIGENZA ARTIFICIALE (IA) IN AZIENDA

Stato delle edizioni

Edizione n°	Motivo della edizione	Data
1	Prima emissione	10/06/2026

Approvazione ed emissione

	Data	Firma
Verificato ed approvato – C.d.A. AMAG Deliberazione n. 136	08/05/2026	Il legale rappresentate Dott. Stefano Franciolini
Verificato ed approvato – C.d.A. SO.GE.R.I	12/05/2026	Il legale rappresentat Ing. Mauro Bressan
Verificato ed approvato Determina Amag Reti Gas n. 31	11/06/2026	Il legale rappresentate Dott. Andrea Biancato

Sommario

1. **Premessa** 3

2. **Ambito di applicazione** 5

3. **Rischi generali di applicazione dell'IA** 5

4. **Principi generali per il corretto utilizzo di tool di AI** 6

5. **Obblighi per il personale** 7

6. **Presidi e tutele legali** 9

7. **Sicurezza Informatica** 12

8. **Formazione e sensibilizzazione** 13

9. **Norme per la proposta di nuovi tool all'interno del Gruppo Gruppo Amag** 13

10. **Note conclusive, violazione della policy e sanzioni** 13

11. **Aggiornamenti e revisione** 13

1. Premessa

Il presente regolamento definisce le modalità di gestione e le limitazioni relative all'utilizzo di strumenti di Intelligenza Artificiale all'interno del Gruppo Amag, in conformità al Regolamento (UE) 2016/679 (GDPR), al D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018, nonché alle normative europee e nazionali vigenti in materia di protezione dei dati personali, sicurezza informatica e sistemi di Intelligenza Artificiale.

L'Intelligenza Artificiale rappresenta una tecnologia in continua evoluzione che può comportare benefici operativi ma anche rischi significativi, in particolare in relazione a:

- sicurezza delle informazioni;
- protezione dei dati personali;
- tutela del know-how aziendale;
- rispetto degli obblighi normativi;
- protezione dell'immagine aziendale.

Per tali ragioni, il Gruppo Amag stabilisce che l'utilizzo di strumenti di Intelligenza Artificiale non è consentito all'interno dell'azienda, salvo specifica autorizzazione formale rilasciata dalla Direzione aziendale.

La sicurezza delle informazioni e dei dati aziendali costituisce una priorità assoluta per il Gruppo Amag e prevale su qualsiasi potenziale vantaggio derivante dall'utilizzo di strumenti basati su Intelligenza Artificiale.

1.1 Obiettivo del Documento

Il presente regolamento ha lo scopo di:

- vietare l'utilizzo non autorizzato di strumenti di Intelligenza Artificiale;
- prevenire rischi legati alla diffusione di informazioni aziendali;
- tutelare i dati personali trattati dall'azienda;
- proteggere il know-how aziendale;
- garantire il rispetto della normativa vigente;
- promuovere comportamenti responsabili nell'utilizzo delle tecnologie digitali.

La presente policy si integra con:

- il Disciplinare per l'utilizzo degli strumenti informatici;
- le policy aziendali sulla sicurezza informatica;
- le policy sulla protezione dei dati personali;

1.2 Definizione rilevanti

Ai fini della presente Policy devono considerarsi le definizioni che seguono:

Brand si tratta di una combinazione di elementi (es. nome, logo, reputazione) che fungono da segno distintivo ed esclusivo di un'azienda. Il brand caratterizza l'azienda e la distingue dai competitor, per questo racchiude in sé l'immagine e la notorietà aziendale. Il Gruppo Amag in particolare, si distingue per essere una azienda in grado di rappresentare l'eccellenza italiana ed è per questo esponente di un insieme di valori diffusi (da riferirsi specificamente alla propria storia).

Credenziali di Autenticazione le informazioni o i dispositivi assegnati in via esclusiva all'Incaricato/dipendente per accedere a determinati Dati personali (es. user name e password, badge o pin, token, etc.).

Dato qualunque dato o informazione personale e aziendale, nonché ogni ulteriore informazione relativa a Gruppo Amag, al business e all'attività che svolge, anche quando non ha carattere personale.

Informazioni riservate o confidenziali tutte le informazioni, i dati, le formule, i processi, le procedure, i metodi, le documentazioni, i disegni, i progetti, gli schemi, le specifiche, i prototipi, i risultati di test, le valutazioni, il know-how ed altri diritti di proprietà intellettuale, le licenze, le informazioni circa la ricerca e lo sviluppo, i business plan, gli elenchi fornitori, gli elenchi di clienti e le informazioni circa i clienti, nonché in generale qualsiasi altro materiale direttamente o indirettamente riferito ad attività commerciali, beni, prodotti, processi o prospetti di proprietà del Gruppo Amag che vengono utilizzate, comunicate, fornite o osservate da tutti i componenti dell'organizzazione aziendale direttamente o indirettamente, in qualsiasi momento o modo siano esse ricevute, che siano destinate ad un uso unicamente interno.

Digital Content detto anche contenuto digitale, si tratta di qualsiasi contenuto esistente sotto forma di dati digitali, come testi, immagini, video e audio condivisi/diffusi/apprezzati mettendo "mi piace" o aggiungendo altre reazioni tramite piattaforme online o device. È archiviato su memoria digitale o analogica in formati specifici.

Password metodo di autenticazione che permette l'accesso in modo esclusivo ad un device, può essere effettuata anche attraverso più fattori (c.d. multifactor authentication o strong authentication) che oltre ad una sequenza di caratteri alfanumerici (es. PIN, password ecc.) richiede l'utilizzo di un device (es. token, smartphone ecc.) o di un dato particolare (es. impronta digitale, riconoscimento facciale, iride etc.).

Risorse Informatiche il personal computer (fisso o portatile), le periferiche, gli hard disk esterni e altri dispositivi di storage, i software, le banche dati, le reti informatiche e dispositivi di comunicazione audio/video e collaborazione, il fax, la posta vocale, i telefoni fissi e mobile, i palmari, i tablet, l'accesso ad internet, le utenze di posta elettronica, le apparecchiature IoT, gli assistenti vocali basati su AI o sistemi Co-pilot ed ogni altra attrezzatura o tecnologia per il trattamento di dati in formato elettronico messa a disposizione dal Gruppo Amag.

Sicurezza informatica è l'insieme di mezzi, tecnologie e procedure volti alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici. Le misure di sicurezza sono, dunque, quelle misure tecniche ed organizzative a protezione dei dati trattati che, secondo

quanto stabilito dall'art. 32 del GDPR, devono essere messe in atto dal titolare e dal responsabile del trattamento tenendo conto dello stato dell'arte, dei costi di attuazione, della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche dei rischi per i diritti e le libertà delle persone fisiche.

Utente /User tutti i soggetti che interagiscono mediante AI, device o più in generale Risorse informatiche e digitali.

Dati personali: qualsiasi informazione relativa a una persona fisica identificata o identificabile ("interessato"), quali, a mero titolo esemplificativo: nome, cognome, indirizzo, numero di telefono, indirizzo e-mail, ecc.

Trattamento: qualsiasi operazione o insieme di operazioni compiute su Dati personali o su insiemi di Dati personali;

Sistema/Tool di AI/IA: un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali;

AI/IA Generativa: un Sistema di IA specificamente destinato a generare, con vari livelli di autonomia, contenuti quali testi complessi, immagini, audio o video.

2. Ambito di applicazione

Rientrano nell'ambito di applicazione della presente policy tutti i tool di AI da parte di tutti i dipendenti, collaboratori, consulenti, fornitori, stagisti e terze parti.

A titolo esemplificativo e non esaustivo non sono consentiti i seguenti utilizzi dell'IA:

I. ChatGPT o altro LLM per comunicazione interna o esterna

II. Tool AI per la generazione di immagini per comunicazione interna o esterna

III. Tool AI per la gestione documentale per comunicazione interna o esterna

IV. Tool AI per l'analisi dei rischi per attività riconducibili all'area sicurezza aziendale

V. Tool AI per la trascrizione di call/discorsi/audio/video/etc previe specifiche autorizzazioni e consensi.

Il regolamento si applica a tutto il personale dipendente, collaboratori, consulenti, fornitori e terze parti che, a qualunque titolo, utilizzino sistemi di Intelligenza Artificiale all'interno dell'ecosistema aziendale, sia su strumenti aziendali che personali impiegati per fini lavorativi.

3. Rischi generali di applicazione dell'IA

L'evoluzione dell'intelligenza artificiale ha portato alla luce numerosi casi che mostrano i rischi associati alla sua implementazione e al suo utilizzo, soprattutto in termini di allucinazioni e bias algoritmici.

Le allucinazioni si riferiscono a situazioni in cui un sistema di AI, producendo output che non sono basati sulla realtà o sulla verità oggettiva, genera informazioni fuorvianti o inesatte o che non sono coerenti con i dati di input forniti. I bias algoritmici sono risultati generati dal funzionamento stesso dell'algoritmo che consistono in distorsioni fattuali da cui possono derivare distorsioni etiche, oppure causati dall'omissione e non considerazione di informazioni e istruzioni fornite dall'utente.

Alcuni esempi tratti da circostanze realmente verificatesi evidenziano l'importanza di una gestione attenta e responsabile delle tecnologie di AI:

- traduzioni errate: può accadere che frasi in un linguaggio sorgente vengono tradotte dal tool in modo completamente errato nel linguaggio di destinazione, talvolta inserendo contenuti non presenti o distorcendo il significato originale.

- Generazione di notizie false: può accadere che il tool menzioni eventi inesistenti o riporti dichiarazioni distorte, provocando confusione o danni alla reputazione.

- Generazione di immagini distorte: può accadere che i tool invitato a generare immagini da descrizioni testuali crei oggetti inesistenti o combinazioni bizzarre di elementi, non corrispondenti alle richieste degli utenti.

- Bias di genere o razziale: può accadere che sistema di riconoscimento facciale abbia maggiori difficoltà nel correttamente identificare persone di certe etnie o generi, dovuto a una rappresentazione non equilibrata nei set di dati di addestramento; o che un sistema di riconoscimento vocale mostri difficoltà nel comprendere accenti non standard o dialetti, portando a una qualità del servizio inferiore per utenti di determinate aree geografiche o gruppi etnici.

- Bias in sistemi di assunzione e reclutamento: può accadere che algoritmi utilizzati per filtrare candidati mostrino preferenze per soggetti di un certo genere o background, basandosi su pattern non eticamente validi presenti nei dati storici.

- Errori in sistemi di assistenza medica: può accadere che un sistema finalizzato ad assistere nelle diagnosi mediche mostri limitazioni, ad esempio, non riuscendo a identificare correttamente patologie rare o interpretando erroneamente immagini mediche a causa di pattern imprevisti nei dati.

- Bias razziale in algoritmi di condanna giudiziaria: può accadere che un sistema utilizzato per valutare il rischio di recidiva sovrastimi il rischio per gli imputati di una certa provenienza etnica, influenzando le decisioni sui loro casi.

Per tal ragioni è necessario attuare misure di prevenzione atte a non generare informazioni forvianti e/o errate all'interno dell'azienda.

4. Principi generali per il corretto utilizzo di tool di AI

L'utilizzo di strumenti di Intelligenza Artificiale (IA) è vietato all'interno delle società del Gruppo AMAG S.p.A., salvo nei casi in cui sia stata preventivamente rilasciata una specifica autorizzazione scritta.

Le richieste di autorizzazione all'utilizzo di strumenti di IA devono essere presentate per iscritto all'Ufficio Privacy, il quale, congiuntamente al reparto IT, provvederà a valutarne i presupposti, i rischi e le modalità di impiego. A seguito dell'analisi, saranno predisposte apposite autorizzazioni operative conformi alle normative vigenti e alle politiche aziendali.

La documentazione predisposta sarà successivamente sottoposta all'esame e all'approvazione del Legale Rappresentante della società del Gruppo AMAG presso cui il richiedente presta servizio.

Nell'utilizzo professionale degli strumenti di AI è necessario seguire linee di condotta coerenti con i seguenti principi fondamentali:

Responsabilità: se state utilizzando un tool di AI del Gruppo Amag fatelo in modo responsabile e corretto. Il vostro comportamento può infatti avere conseguenze – positive e negative – non solo su voi stessi ma anche sul Gruppo Amag. È fondamentale adottare un approccio etico e consapevole durante l'attività di prompting e in generale nell'uso dell'AI. Quindi, sia nel formulare le istruzioni, sia nel verificare l'output, l'utente ha sempre l'obbligo di controllare che non vengano violate normative vigenti o policy aziendali. È necessario utilizzare i tool di AI solo per scopi e nei limiti consentiti. Un uso improprio può esporre il Gruppo Amag a rischi legali, etici e di reputazione

Riservatezza: le informazioni confidenziali e i segreti industriali relativi all'attività del Gruppo Amag sono riservati e non possono essere divulgati se non espressamente autorizzati. Per questa ragione è assolutamente vietato utilizzare immagini, video, voci e contenuti di team, persone o dettagli in ufficio per strumenti di AI che non siano autorizzati o di cui non ne sia autorizzato l'uso da parte del Gruppo Amag. In caso di dubbi, è sempre possibile consultare l'Ufficio Privacy.

L'utilizzo di strumenti di IA deve comunque sempre rispettare i seguenti principi:

- Liceità, correttezza e trasparenza nel trattamento dei dati.
- Limitazione della finalità: l'uso dell'IA deve essere coerente con le finalità per cui è stato autorizzato.
- Minimizzazione dei dati: devono essere utilizzati solo i dati strettamente necessari.
- Integrità e riservatezza: garantire un adeguato livello di sicurezza dei dati trattati.
- Responsabilità e tracciabilità: ogni utilizzo deve essere documentabile e riconducibile a un soggetto autorizzato.

5. Obblighi per il personale

Anche sulla base di questi principi è importante essere consapevoli dell'importanza delle seguenti regole di condotta e obblighi da parte di tutti i soggetti autorizzati nell'utilizzo di strumenti di AI:

1. al momento della registrazione a un servizio o dell'adesione a un tool di AI, si accettano i termini e le condizioni d'uso del servizio stesso. Pertanto, è cruciale comprendere chiaramente le disposizioni previste, poiché la violazione di tale policy può comportare conseguenze legali significative;

2. è fondamentale non inserire nei tool di AI pubblici o comunque non autorizzati dal Gruppo Gruppo Amag, informazioni confidenziali o riservate, quali: informazioni di clienti o fornitori, registrazioni di call, questionari, know-how aziendale, etc. (vedasi paragrafo sulle definizioni);

3. è possibile utilizzare informazioni confidenziali o riservate unicamente in tool di AI autorizzati dall'azienda, entro i limiti e per gli scopi approvati dall'azienda;

4. in generale tutte le informazioni, i dati, gli input, i contenuti caricati oppure utilizzati per l'attività di prompting, devono rappresentare una fonte corretta ed efficace per lo strumento in uso;

5. È obbligatorio valutare la qualità del lavoro svolto mediante l'utilizzo di strumenti di AI (output), assicurandosi che non contenga errori, contenuti discriminatori o comunque contrari ai valori del Gruppo Amag, l'AI non può mai essere utilizzata come unica fonte di sapere o di verità e ogni output deve essere verificato per attendibilità e utilizzabilità prima di essere condiviso;

6. È necessario verificare, ove ciò sia possibile, che gli output forniti dai sistemi di AI non violino diritti di proprietà intellettuale o diritti d'autore di terze parti;

7. Non è ammesso, per i tool messi a disposizione a livello aziendale, un uso diverso da quello lavorativo; i dipendenti non dovranno ritenere privati o personali le informazioni, gli output, i documenti e i dati trattati e memorizzati mediante l'uso di tool di AI adottati da Gruppo Amag; tutti i contenuti sono infatti di proprietà di Gruppo Amag;

8. Se per errore si carica, cioè si inserisce o si trasferisce, un contenuto inappropriato su un tool di AI, è fondamentale rimuoverlo nel più breve tempo possibile;

9. Non è ammesso l'uso di materiale illecito (parole, immagini o contenuti) o che possa essere percepito come imbarazzante, offensivo, falso, molesto o diffamatorio nei confronti di qualsiasi persona o entità e non deve mai essere utilizzato per prompting o in generale per strumenti AI;

10. È vietato utilizzare strumenti di AI per la produzione di materiale illecito (testi, immagini o contenuti di qualsiasi natura), né per generare contenuti prodromici alla commissione di illeciti;

11. Non devono essere utilizzati dati personali, immagini, audio e video senza il consenso del soggetto interessato o senza idonea base giuridica, perché ciò può rappresentare un illecito civile o addirittura penale;

12. È vietato utilizzare strumenti di AI in modo che possano generare discriminazioni di qualsiasi tipo basate su razza o origine etnica, orientamento sessuale, stato di salute, disabilità, età, religione o qualsiasi altra caratteristica personale;

13. È vietato utilizzare strumenti di AI per creare, generare o diffondere materiale falso, ingannevole o manipolato, compresi testi, immagini o video, che possano indurre in errore o alterare la veridicità delle informazioni o compromettere la reputazione delle persone o del Gruppo Amag;

14. È necessario considerare l'intelligenza artificiale solo come un supporto per il processo decisionale e uno strumento per ottimizzare i processi e migliorare l'efficacia operativa; tuttavia, la responsabilità ultima delle decisioni strategiche e delle azioni deve rimanere sotto il controllo umano;

15. L'uso degli strumenti di intelligenza artificiale deve avvenire nel pieno rispetto delle normative vigenti, tra cui quelle relative alla privacy e protezione dei dati personali, alla tutela del diritto d'autore e alla sicurezza informatica.

16. Non delegare ad algoritmi di IA processi decisionali critici in assenza di supervisione umana, in particolare se tali decisioni producono effetti giuridici o incidono significativamente su individui.

17. Non utilizzare sistemi di IA per attività di monitoraggio occulto o controllo a distanza di altri dipendenti.

18. Segnalare immediatamente eventuali violazioni di sicurezza (data breach) o comportamenti anomali dei sistemi IA alla funzione IT e all'Area Privacy.

19. Utilizzare esclusivamente strumenti e piattaforme di IA espressamente autorizzate dal Gruppo Amag. Qualsiasi nuovo strumento deve essere oggetto di una valutazione preliminare dei rischi (DPIA) e approvato per l'uso.

6. Presidi e tutele legali

6.1 Riservatezza e compliance GDPR e IA Act

Dal punto di vista della riservatezza aziendale, è necessario evitare di utilizzare (i) contenuti che possano ledere il diritto alla riservatezza di colleghi o di terzi in genere, (ii) informazioni riservate aziendali o segreti industriali o commerciali, (iii) informazioni su clienti, partner commerciali o fornitori, perché questa categoria di dati è considerata strategica.

Inoltre, è importante tenere a mente che qualsiasi utilizzo che comporti trattamento di dati personali determina la necessità di garantire la compliance con il Regolamento in materia di protezione dei dati personali ("GDPR").

Ciò significa che dobbiamo sempre assicurarci che:

- sia individuata una base giuridica consona;
- siano fornite adeguate informazioni agli interessati;
- siano trattati i dati personali strettamente necessari rispetto alla finalità;
- siano conservati i dati personali secondo le tempistiche previste da Gruppo Amag;
- sia sempre presente una supervisione e/o un controllo umano prima che l'*output* comporti decisioni concernenti gli interessati.

Per queste motivazioni, quando possibile, occorre evitare di utilizzare dati personali quando si utilizzano strumenti di AI aziendali.

E' comunque sempre vietato il caricamento di documenti aziendali riservati (contratti, progetti, dati contabili, documentazione tecnica) in strumenti IA non aziendali o con server ubicati fuori dallo Spazio Economico Europeo.

Infine, è importante conoscere il ruolo di Gruppo Amag così come sancito dal Regolamento sull'Intelligenza Artificiale ("AI Act").

Risulta fondamentale che tutte le comunicazioni riguardanti le tecnologie di IA siano gestite in modo controllato e autorizzato. Pertanto, è vietato pubblicare informazioni, dettagli o commenti sui social media o su qualsiasi altra piattaforma online riguardanti i nostri sistemi di IA senza previa autorizzazione esplicita da parte di Gruppo Amag.

6.2 Rispetto delle norme sul diritto d'autore

Il diritto d'autore è una tutela legale che protegge le opere d'ingegno originali. Questo diritto si applica automaticamente dal momento della creazione dell'opera, senza necessità di registrazione formale, e copre una vasta gamma di opere, tra cui:

- opere visive o audiovisive: video, film, programmi, videogiochi, dipinti, fotografie, immagini, grafiche;
- contenuti audio: composizioni musicali, registrazioni sonore, registrazioni di discorsi, clip;
- testi: libri, manoscritti, articoli, saggi, codici sorgente, algoritmi.

Il diritto d'autore non protegge i fatti o le idee in sé, ma solo la specifica espressione di tali fatti o idee. Questo implica che è possibile esprimere la stessa idea o fatto in modi diversi, purché non si copi la particolare espressione altrui. Per beneficiare della protezione offerta dal diritto d'autore, inoltre, un'opera deve essere originale. Questo significa che l'opera deve essere:

- creata dall'autore in prima persona: l'opera deve essere il frutto dell'ingegno e dell'espressione personale dell'autore, anche laddove realizzata servendosi di strumenti di AI;
- dotata di un minimo livello di creatività: anche un'opera semplice può essere protetta se contiene elementi di creatività e originalità sufficienti. Non tutte le creazioni possono essere

protette dal diritto d'autore. Nomi, titoli, slogan o frasi brevi generalmente non soddisfano i requisiti di originalità necessari per ottenere tale protezione.

Il rispetto del diritto d'autore non solo protegge il dipendente da potenziali rischi legali, ma sostiene anche l'integrità e l'etica professionale nel nostro ambiente di lavoro.

Di norma, il diritto d'autore appartiene alla persona che crea un'opera originale. Ad esempio, se realizzi autonomamente un testo o una grafica, sei probabilmente il titolare del diritto d'autore di quell'opera. Analogamente, se scatti una fotografia, è probabile che tu ne detenga il diritto d'autore.

Se invece crei un'opera nell'esercizio delle tue normali responsabilità lavorative, anche tramite i tool di AI, potresti non essere il titolare del diritto d'autore. In alcuni casi, la legge attribuisce la titolarità al tuo datore di lavoro, considerandolo l'autore dell'opera ai fini del diritto d'autore.

Il titolare del diritto d'autore ha determinati diritti esclusivi sanciti dalla legge, tra cui, ad esempio:

- il diritto di riproduzione: il titolare può impedire a terzi di copiare la sua opera;
- il diritto di distribuzione: il titolare può controllare la distribuzione e diffusione delle copie della sua opera;
- il diritto di modifica: il titolare può impedire la creazione di opere derivate basate sulla sua opera.

La violazione del diritto d'autore si verifica quando si intraprende una di queste attività senza l'autorizzazione del titolare.

È essenziale rispettare il diritto d'autore quando si intendono utilizzare opere protette come input per i tool di AI. In tal caso, è sempre necessario:

- Non utilizzare opere senza autorizzazione: è responsabilità del dipendente evitare di utilizzare in tutto o opere protette senza autorizzazione del titolare (ad esempio Gruppo Amag, i clienti di Gruppo Amag oppure terzi che ne detengono i diritti di sfruttamento), anche se le idee sottostanti possono essere le stesse. Questo significa che è vietato utilizzare come input per i tool di AI testi, immagini, suoni o altri contenuti protetti senza il permesso del titolare;
- Verificare la licenza delle opere utilizzate: è responsabilità del dipendente assicurarsi di detenere le necessarie licenze sulle opere utilizzate come input per i tool di AI, che ne permettono l'uso anche per fini di addestramento del sistema adoperato;
- Utilizzare preferibilmente opere nel pubblico dominio: è preferibile, nel caso, utilizzare opere che sono nel pubblico dominio o che sono coperte da licenze aperte (come Creative Commons) che permettono l'uso senza restrizioni, al fine di evitare contestazioni legali;
- Monitorare e documentare: è opportuno mantenere un registro accurato delle opere utilizzate, incluse le informazioni sulle licenze e le autorizzazioni ottenute, per dimostrare la conformità alle normative sul diritto d'autore;

- Attribuire correttamente i crediti: quando si utilizzano opere protette da licenza che richiedono l'attribuzione, è necessario fornire correttamente i crediti richiesti all'autore originale, seguendo le modalità specificate nella licenza;

- Evitare presunzioni di non violazione: non bisogna presumere che l'uso di contenuti protetti sia ammissibile solo perché il materiale è stato modificato, acquistato legalmente, trovato su Internet, o perché altri hanno utilizzato contenuti simili;

- Consultare preventivamente responsabile in caso di incertezza riguardo l'utilizzo di opere protette all'interno di progetti che coinvolgono tool di AI è opportuno, ove possibile, consultare il reparto legale di Gruppo Amag per evitare violazioni involontarie del diritto d'autore;

- Aggiornamento: è dovere di ogni dipendente aggiornarsi costantemente sulle politiche aziendali relative all'uso di sistemi di AI, comprendendo che queste sono formulate per proteggere sia Gruppo Amag che i suoi dipendenti da rischi legali e reputazionali e per garantire che l'utilizzo dei tool di AI sia sempre conforme alle normative vigenti; corsi di formazione ad hoc verranno messi a disposizione per l'intera organizzazione aziendale.

7. Sicurezza Informatica

La legislazione internazionale e nazionale impone specifichi obblighi in materia di sicurezza informatica e protezione dalle minacce informatiche in rapida e continua evoluzione, in ambito di protezione dati e sicurezza dati. È, inoltre, prescritto che i piani di Cyber Security e i relativi modelli di valutazione debbano essere definiti rispetto alla struttura organizzativa aziendale, al settore di attività e allo stato delle minacce esterne. Il core business del Gruppo Amag lo pone nel mirino dei criminali informatici e per questa ragione, oltre al modello di compliance privacy, esistono specifiche misure di sicurezza propedeutiche alla protezione dei dati aziendali.

Sul punto si intendono integralmente richiamati il Disciplinare per l'utilizzo degli strumenti informatici, di internet e della posta elettronica del Gruppo Amag già adottato in azienda per l'utilizzo delle risorse informatiche e telematiche aziendali. Infatti, in base al principio di "accountability" previsto dall'art. 24 del GDPR, le norme sulla protezione dei dati personali sanzionano la società che non abbia predisposto idonee difese contro qualsiasi aggressore. Questo può accadere nel caso in cui non sia stato rispettato l'obbligo di implementare misure di sicurezza adeguate alla tutela dei dati, ai sensi dell'art. 32 GDPR, con la conseguenza – anche non immediata - che anche una disattenzione da parte del dipendente può rappresentare un rischio per l'intera azienda. Il rischio sanzionatorio è molto elevato, con conseguenze anche gravi, perché le sanzioni del Garante Privacy possono arrivare fino a 20 milioni di euro e possono essere pari al 2% o al 4% del fatturato aziendale.

A tal proposito, ai sensi degli articoli 29 e 32 del GDPR, il datore di lavoro impartisce istruzioni e aggiornamenti anche con riferimento alle modalità del trattamento effettuato tramite soluzioni che si basino su intelligenza artificiale. Per questa ragione, non solo la policy per l'utilizzo delle risorse informatiche prescrive una serie di norme per l'utilizzo corretto dei device per soli scopi lavorativi. Ogni eventuale responsabilità per danni anche indirettamente causati a Gruppo Amag sarà ricondotta direttamente al comportamento degli Utenti.

La gestione di eventuali account di strumenti di AI dovrà dunque essere improntata alle disposizioni di sicurezza ed alle norme di comportamento indicate dal Gruppo Amag.

8. Formazione e sensibilizzazione

La formazione nell'utilizzo di strumenti di IA è fondamentale per consentire un utilizzo adeguato ed efficace di tali strumenti, pertanto la partecipazione ad attività formative promesse dalle aziende del Gruppo Amag sulla tematica oggetto del presente regolamento sarà obbligatoria per tutte le figure che utilizzano strumenti IA nell'esercizio delle proprie mansioni.

9. Norme per la proposta di nuovi tool all'interno del Gruppo Gruppo Amag

Nel caso in cui il dipendente volesse adottare un tool IA è possibile inviare una e-mail agli indirizzi ced@gruppoGruppo Amag.it e risorseumane@gruppoGruppo Amag.it

La proposta verrà valutata nel più breve tempo possibile ed ognuna verrà riscontrata con accettazione/rifiuto/modifica.

A seguito dell'esito verranno svolti ulteriori step di test e validazione delle soluzioni di AI proposte, al fine di verificare che questi in effetti abbiano le funzionalità previste e rispettino tutti i requisiti aziendali e normativi.

Ogni strumento di IA esterno al perimetro aziendale e che non sia stato formalmente approvato per l'uso da parte del Gruppo Amag deve ritenersi totalmente vietato.

10. Note conclusive, violazione della policy e sanzioni

Violazioni del presente regolamento saranno oggetto di accertamento da parte delle competenti funzioni aziendali. A seconda della gravità, potranno essere adottati provvedimenti disciplinari in conformità con il CCNL Utilitalia Gas- Acqua e con il Codice Disciplinare aziendale, fermo restando il possibile coinvolgimento delle autorità competenti in caso di reati informatici o violazioni del GDPR.

11. Aggiornamenti e revisione

Il presente regolamento potrà essere aggiornato a seguito di evoluzioni normative, tecnologiche o organizzative. Ogni modifica sarà comunicata formalmente a tutto il personale.