Regolamento aziendale Sotacarbo SpA

REGOLAMENTO PER L'UTILIZZO AZIENDALE DELL'INTELLIGENZA ARTIFICIALE GENERATIVA (GenAI)

1. Obiettivi e quadro normativo di riferimento

1. Il presente regolamento stabilisce le regole per l'utilizzo sicuro, etico e conforme dei sistemi di Intelligenza Artificiale (IA) in azienda. L'obiettivo è favorire l'innovazione tecnologica salvaguardando il patrimonio informativo aziendale (*know-how*), i diritti di proprietà intellettuale e i dati personali.
2. Il documento si adegua ed è vincolato alle seguenti normative:

- **Regolamento (UE) 2024/1689** (Definito l'**EU AI Act**), con focus sugli obblighi di trasparenza del Capo IV e le scadenze di compliance previste per il 2 agosto 2026. A tale proposito si precisa che le disposizioni relative ai sistemi di IA ad alto rischio di cui all'Allegato III dell'AI Act diventano applicabili il 2 agosto 2026. Entro tale data, la Società deve: (i) completare la mappatura dei sistemi ad alto rischio in uso; (ii) adottare un sistema di gestione della qualità per ciascuno di essi; (iii) completare le DPIA eventualmente necessarie. Il mancato adempimento espone la Società alle sanzioni di cui all'art. 99 dell'AI Act.
- **Legge n. 132/2025** (Legge Italiana sull'Intelligenza Artificiale).
- **Regolamento (UE) 2016/679 (GDPR)** relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali.
- **D.Lgs. 30/2005** (Codice della Proprietà Industriale) in materia di tutela del segreto commerciale e industriale.
- **D.Lgs. 231/2001** in materia di responsabilità amministrativa degli enti.

2. Ambito soggettivo e oggettivo di applicazione

A. **Ambito Soggettivo:** Il regolamento si applica obbligatoriamente a chiunque svolga attività in nome o per conto dell'azienda, indipendentemente dalla natura del rapporto contrattuale.
B. **Ambito Oggettivo:** Si applica a qualsiasi sistema software basato su modelli linguistici di grandi dimensioni (LLM), generatori di immagini, codice software, audio o video (es. ChatGPT, Microsoft Copilot, Midjourney, Claude) integrato nei processi aziendali o utilizzato tramite dispositivi aziendali.

3. Classificazione e governance degli strumenti (IL "SEMAFORO")

L'azienda suddivide i software di IA Generativa in tre categorie di utilizzo:

Categoria	Descrizione	Regole di Utilizzo	Esempi Pratici
🟢 **VERDE (Approvati)**	Strumenti commerciali con licenza aziendale e	**Uso Autorizzato.** I dati inseriti non vengono utilizzati per	Microsoft Copilot Enterprise, ChatGPT

	clausole di protezione dati verificate.	l'addestramento dei modelli esterni.	Team/Enterprise, LLM On-Premise.
🟡 **GIALLO (Sotto Esame)**	Strumenti utili a specifici reparti ma non ancora contrattualizzati a livello centrale.	**Richiesta preventiva.** È necessario il nullaosta del Responsabile IT e del DPO prima dell'accesso.	Plugin specialistici di traduzione o generazione di codice di terze parti.
🔴 **ROSSO (Vietati)**	Strumenti "consumer", gratuiti o privi di garanzie legali di riservatezza.	**Blocco Tecnologico.** È vietato l'accesso tramite credenziali aziendali o per scopi di lavoro.	ChatGPT versione gratuita, Midjourney/DALL-E su account personali.

3-bis. Registro degli Strumenti di IA

L'addetto ai sistemi informatici, su indicazione del DPO, mantiene un registro aggiornato di tutti gli strumenti di IA in uso o in fase di valutazione, contenente: denominazione e versione del sistema, categoria di rischio assegnata (verde/giallo/rosso), fornitore, finalità d'uso, tipologia di dati trattati, esito della valutazione di conformità. Il registro è pubblicato nella sezione 'Amministrazione Trasparente' del sito istituzionale, nella misura richiesta dall'art. 30, comma 5, del D.Lgs. 36/2023, ed è messo a disposizione del Garante su richiesta

4. Tutela del segreto industriale e del know-how

1. Al fine di preservare il vantaggio competitivo aziendale e prevenire la fuga accidentale di dati proprietari (*data leak*), è tassativamente vietato immettere nei "prompt" o caricare (upload) come allegati:
   - Codici sorgente di software proprietari non rilasciati pubblicamente.
   - Piani di business, strategie di marketing e di posizionamento sul mercato.
   - Dati finanziari storici o previsionali (bilanci non ancora pubblici).
   - Informazioni relative a brevetti, prototipi o segreti industriali coperti da un NDA (Non-Disclosure Agreement).
2. L'inserimento di questi dati all'interno di strumenti a "Semaforo Rosso" comporta la perdita del requisito di segretezza legale del Know-How.

5. Compliance privacy e trattamento dati (GDPR)

1. L'utilizzo dell'IA generativa deve rispettare fedelmente il principio di **Minimizzazione dei dati** (Art. 5, par. 1, lett. c del GDPR):

   a) Prima di inserire qualsiasi testo o documento nei sistemi di IA, il dipendente deve provvedere alla rimozione o mascheramento di dati personali (es. nomi, cognomi, e-mail, numeri di telefono, codici fiscali).

b) È vietato il trattamento tramite IA di dati ex art. 9 GDPR (sanitari, biometrici, opinioni politiche o sindacali) salvo esplicita e preventiva Valutazione di Impatto sulla Privacy (DPIA) redatta dal DPO aziendale. Laddove si dovesse rendere necessaria la DPIA per sistemi di IA essa è redatta dal DPO avvalendosi del modello di questionario predisposto ai sensi dell'art. 27, par. 5, dell'AI Act [AI ACT]. Per i sistemi classificati ad alto rischio ai sensi dell'Allegato III dell'AI Act, la DPIA integra altresì la valutazione d'impatto sui diritti fondamentali di cui all'art. 27 dell'AI Act [AI ACT]. Nessun sistema classificato ad alto rischio può essere messo in uso senza previa DPIA approvata dal Titolare.

c) Qualsiasi utilizzo di sistemi di IA finalizzato alla selezione dei candidati, alla valutazione delle performance o all'assegnazione dei compiti ricade nell'**Alto Rischio** ai sensi dell'AI Act. Tali sistemi richiedono una procedura di approvazione rafforzata e non possono operare in totale autonomia. Sotacarbo Spa (deployer) non adotta sistemi di IA per la selezione dei candidati, per la valutazione delle performance o per l'assegnazione dei compiti. Laddove dovessero adottati, rientrando essi nei sistemi ad alto rischio, il deployer in base a quanto stabilito dall'art 26 AI Act dovrà assolvere ai seguenti obblighi:
   - Adottare misure tecniche e organizzative per l'uso conforme;
   - Effettuare una valutazione d'impatto sui diritti fondamentali (art. 27 AI Act) per i sistemi di cui all'Allegato III, punto 4 (sistemi IA nell'occupazione);
   - Garantire la supervisione umana durante l'utilizzo;
   - Registrare i log automatici generati dal sistema, ove tecnicamente possibile;
   - Notificare incidenti gravi alle autorità competenti.

   In tal caso il presente Regolamento dovrà essere aggiornato traducendo quanto sopra in adeguate procedure operative.

2. Qualora un trattamento effettuato mediante strumenti di IA sia basato sul legittimo interesse del Titolare e preveda l'uso di nuove tecnologie o strumenti automatizzati, il DPO trasmette una comunicazione preventiva al Garante per la protezione dei dati personali ai sensi dell'art. 1, comma 1022, L. 205/2017, prima dell'avvio del trattamento.

5.1 Utilizzo di sistemi di IA nelle procedure di approvvigionamento

In qualità di stazione appaltante soggetta al D.Lgs. 36/2023, Sotacarbo S.p.A. garantisce che eventuali strumenti algoritmici o di IA utilizzati nell'ambito delle procedure di gara rispettino i principi di: (a) conoscibilità e comprensibilità, con obbligo di informare gli operatori economici dell'esistenza di processi decisionali automatizzati e della logica utilizzata; (b) non esclusività della decisione algoritmica, con contributo umano di controllo e validazione; (c) non discriminazione algoritmica, con misure tecniche e organizzative adeguate. L'elenco delle soluzioni tecnologiche algoritmiche utilizzate è pubblicato sul sito istituzionale, nella sezione 'Società Trasparente', ai sensi dell'art. 30, comma 5, D.Lgs. 36/2023.

6. Supervisione umana e responsabilità

I dipendenti sono informati che:

- i sistemi di IA generativa sono soggetti ad "**allucinazioni algoritmiche"** (generazione di fatti falsi ma verosimili);
- l'operatore umano rimane l'unico e definitivo responsabile della correttezza, accuratezza e conformità legale del lavoro prodotto;

- è fatto obbligo al dipendente di verificare puntualmente le fonti, le cifre e la sintassi del testo o del codice generato prima di qualsiasi utilizzo operativo o invio a soggetti esterni (clienti/fornitori);
- nessun processo decisionale che produca effetti giuridici sul personale o su terzi può essere delegato interamente a un sistema di IA (Art. 22 GDPR).

7. Obliggo di trasparenza e etichettatura

In ottemperanza all'Articolo 50 dell'AI Act europeo, l'azienda implementa la trasparenza verso l'esterno:

- Se un testo, un'immagine, un video o un file audio destinato a clienti, partner o autorità pubbliche è stato generato o significativamente alterato da un sistema di IA, deve contenere un'indicazione esplicita (es. *"Contenuto realizzato con il supporto di sistemi di Intelligenza Artificiale"*);
- È vietata la rimozione manuale o informatica dei sistemi di identificazione (*Watermark*) inseriti nativamente dai software di generazione multimediale;
- In aggiunta a quanto sopra:
  - (i) i deployer di sistemi di riconoscimento delle emozioni o di categorizzazione biometrica informano le persone fisiche esposte del funzionamento del sistema;
  - (ii) i contenuti 'deep fake' generati o manipolati artificialmente devono essere espressamente segnalati come tali, salvo usi artistici o satirici manifestamente riconoscibili come tali [AI ACT].

7.1. Obblighi verso i lavoratori

In base a quanto stabilito dall'art 11 della Legge 132/2025 *«Il datore di lavoro o il committente è tenuto a informare il lavoratore dell'utilizzo dell'intelligenza artificiale nei casi e con le modalità di cui all'articolo 1-bis del decreto legislativo 26 maggio 1997, n. 152».* In accordo con esso non possono essere utilizzati sistemi di IA che consentano il controllo a distanza dei lavoratori così come stabilito dall'art 4 dello Statuto dei Lavoratori, è altresì vietato l'utilizzo di sistemi di IA per decisioni automatizzate che producano effetti giuridici sui lavoratori senza supervisione umana.

8. Gestione degli incidenti IA

1. Laddove vengano utilizzati sistemi di IA classificati come ad alto rischio, l'art 73 dell'AI Act prevede l'obbligo di segnalazione degli eventuali incidenti gravi. Ai fini dell'AI Act (Regolamento UE 2024/1689), un incidente grave è definito all'articolo 3 (punto 49) come qualsiasi evento o malfunzionamento di un sistema di intelligenza artificiale che, direttamente o indirettamente, causi la morte o un danno grave alla salute, una compromissione irreversibile di infrastrutture critiche, violazioni dei diritti fondamentali, danni seri alla proprietà o all'ambiente.
2. Il fruitore (deployer) non deve necessariamente qualificare l'evento come "incidente grave" ma deve monitorare il sistema sul campo con l'obbligo di segnalare:

- Incidenti riscontrati: Qualsiasi malfunzionamento, anomalia o comportamento imprevisto dell'IA.
- Sospetti di rischio: Qualsiasi situazione in cui l'uso del sistema presenti un rischio per la salute, la sicurezza o i diritti fondamentali delle persone.

- Scostamenti dall'uso previsto: Se l'incidente è derivato da una discrepanza tra le istruzioni d'uso del fornitore e il comportamento effettivo dell'algoritmo.

3. Laddove si verifichi l'evento, il flusso di notifica deve seguire il seguente schema:
   - BLOCCO IMMEDIATO —► Il fruitore interrompe l'uso del sistema di IA
   - SEGNALAZIONE —► Il fruitore informa immediatamente il FORNITORE
   - CO-NOTIFICA —► Se viene accertato l'incidente grave, il FORNITORE (o il fruitore stesso) notifica l'Autorità di vigilanza del mercato.
4. Lo schema di notifica interna aziendale segue i seguenti passaggi:
   a. Il Dipendente / Operatore che rileva l'anomalia sospende l'uso dell'IA se rileva un rischio o un malfunzionamento e invia una nota interna immediata al Responsabile IT descrivendo l'anomalia;
   b. Il responsabile dei sistemi informatici isola tecnicamente il sistema di IA per impedirne il riavvio accidentale coinvolgendo subito il DPO per valutare l'impatto sui diritti fondamentali e sulla privacy;
   c. Il DPO valuta se l'evento si qualifica come "incidente grave" o violazione dei dati (Data Breach) ai fini GDPR. In caso positivo redige la bozza di notifica tecnica e legale per il vertice aziendale;
   d. L'Amministratore Unico approva formalmente l'attivazione della procedura di emergenza e autorizza l'invio della segnalazione ufficiale al Fornitore del sistema IA (e, se necessario, all'Autorità di Vigilanza del mercato).

9. Alfabetizzazione

In base alle disposizioni dell'AI Act e della vigente normativa italiana, l'azienda si impegna a fornire adeguata formazione periodica e obbligatoria a tutto il personale per un uso sicuro degli strumenti autorizzati. La mancata partecipazione ai corsi di formazione previsti costituisce inadempimento contrattuale.

10. Controlli e sanzioni

1. La violazione delle disposizioni contenute nella presente Policy mette a rischio la sicurezza e la conformità legale dell'azienda.
2. Costituisce infrazione del Codice Disciplinare aziendale e, a seconda della gravità dell'evento (es. esfiltrazione intenzionale di segreti industriali o sanzioni da parte del Garante Privacy), comporta l'applicazione delle sanzioni previste dal CCNL Elettrico.

11. Coordinamento con gli altri regolamenti

Il presente regolamento si intende da applicarsi coordinatamente con il *Regolamento sulla tutela della privacy* in merito alla disciplina sulla valutazione di impatto DPIA di cui al punto 2 dell'articolo 5 del presente regolamento.

12. Aggiornamento

Il presente regolamento verrà aggiornato laddove dovessero subentrare aggiornamenti di carattere normativo, tecnologico o che comportino modifiche sostanziali alle procedure e alle misure in esso indicate. Tale aggiornamento sarà a cura del DPO in coordinamento con quanti altri possano essere coinvolti.

13. Entrata in vigore

Il presente regolamento entra in vigore con la pubblicazione sul sito web aziendale.

Carbonia, 31/07/2026

Ing. Mario Porcu
Amministratore Unico Sotacarbo SpA

Firmato digitalmente da:
MARIO PORCU
31/07/2026 13:56