Policy di trasformazione digitale

per il Gruppo Tecniplast

Code:	**ESG/GDL07-IT**
Version:	**01.02**
Validity date:	**16.03.26**
Classification:	**PUB -Public**
Type:	**Guideline (Group Policy)**

	Issuance	***Validation***	***Approval***
Role	Group Sust. & DT Director	Sust. Committee (SC)	Sust. Committee (SC)
Name	Roberto Crippa	On behalf of the SC	On behalf of the SC
Signature	*(signed in original)*	Mario Lombardini *(signed in original)*	Alessandro Bernardini *(signed in original)*

Glossario ed acronimi

Vengono utilizzate le seguenti definizioni, acronimi ed abbreviazioni:

IA -Intelligenza Artificiale
Secondo l'EU AI Act, un sistema basato su macchine, progettato per operare con diversi livelli di autonomia e che può mostrare adattabilità dopo il suo impiego e che, per obiettivi espliciti o impliciti, elabora input per generare output come previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali.
L'IA comprende un'ampia gamma di tecnologie, tra cui l'apprendimento automatico, il deep learning e l'elaborazione del linguaggio naturale.

Società
La Società per la quale è in vigore la presente policy, così come indicato dal Comitato di Sostenibilità del Gruppo Tecniplast.

Digital Transformation –Trasformazione digitale
L'adozione e l'implementazione di tecnologie digitali per creare nuovi processi aziendali, prodotti o servizi o migliorare quelli esistenti, allo scopo di aumentare l'efficacia e l'efficienza generando valore aggiunto.

Riferimenti

Un numero racchiuso tra parentesi quadre [n] nel testo fa riferimento alle seguenti fonti di informazione:

[1] "Codice di Condotta del Business del Gruppo Tecniplast", Tecniplast, ESG/GDL01

[2] "EU Artificial Intelligence Act", EU, 2024/1689

[3] "General Data Protection Regulation (GDPR)", EU, 2016/679

Indice

1 Scopo, perimetro di applicazione, destinatari

1.1 Scopo

Scopo della presente *policy* è la definizione di criteri e linee guida atti a garantire che la trasformazione digitale all'interno del Gruppo Tecniplast avvenga nel rispetto dei principi contenuti nel Codice di Condotta [1] e delle applicabili normative internazionali, assicurando in particolare un utilizzo corretto, trasparente e responsabile dell'Intelligenza Artificiale (IA), e vigilando sui potenziali rischi economici e sociali e sull'impatto sui diritti fondamentali e la dignità delle persone.

Poiché la materia è regolata anche da leggi e regolamentazioni locali, le Società interessate adottano le opportune procedure per la sua applicazione.

1.2 Perimetro di applicazione

La presente *policy* si applica alla gestione dei processi di trasformazione digitale della Società ed all'utilizzo dell'IA.

1.3 Destinatari

La presente *policy* è indirizzata tutti i membri della Società, ed in particolar modo agli utilizzatori (*deployer*) e a chiunque abbia la responsabilità di gestire la trasformazione digitale e vigilare sull'utilizzo dell'IA.
Si applica inoltre, ai fornitori della Società che sviluppano e forniscono sistemi e servizi di IA.

2 Introduzione

Il Gruppo Tecniplast promuove lo sviluppo della trasformazione digitale e l'utilizzo dell'IA come strumento per migliorare la produttività ed i processi di business al fine di accrescere la competitività nel pieno rispetto dei diritti umani, delle vigenti leggi in materia e delle *policy* e dei modelli di *governance* adottati.

In coerenza con quanto sopra, la presente *policy* tratta di:

- principi guida che informano la trasformazione digitale e l'utilizzo dell'IA;
- sistemi di gestione dell'IA;
- meccanismi attuativi e di controllo;
- requisiti dei *provider* di IA;
- comportamenti attesi e sanzionabili.

2.1 Classi di rischio

Poiché la trasformazione digitale può coinvolgere l'utilizzo di sistemi di IA, la presente *policy* si conforma alla classificazione di rischio prevista dall' EU AI Act [2] che mira a garantire che i sistemi di IA siano implementati in modo da ridurre al minimo i rischi di danno alla salute, alla sicurezza ed ai diritti fondamentali delle persone.

Più in dettaglio, l'EU AI Act [2] identifica le seguenti classi di rischio:

- **Sistemi di IA a rischio inaccettabile (IA vietata)**
  Vi rientrano tutti i sistemi che possono costituire una chiara minaccia per la sicurezza e i diritti delle persone, o che possono manipolare il comportamento umano, nel tentativo di aggirare il libero arbitrio, o che consentono di attribuire un "punteggio sociale".
  In particolare, sono sistemi volti a:
  - sfruttare le vulnerabilità umane;
  - influenzare, alterare o controllare in maniera esplicita o subliminale il comportamento individuale in modo da alterare l'autonomia di libera scelta inducendo a prendere decisioni che gli individui interessati non avrebbero altrimenti preso;
  - applicare pratiche di social scoring (ossia: valutazione di individui sulla base del loro comportamento, interazioni ed altri dati personali per fini discriminatori od illeciti);
  - applicare pratiche di riconoscimento emotivo nelle aree di lavoro, indipendentemente dal tipo di rapporto lavorativo in essere;
  - applicare pratiche di categorizzazione biometrica basate su caratteristiche sensibili quali razza, opinioni politiche, appartenenza ad organizzazioni sindacali, credenze religiose o politiche, orientamento sessuale;
  - raccolta non mirata di immagini facciali da internet o da telecamere a circuito chiuso per creare database di riconoscimento facciale.

  Note
  1. E' ammesso il riconoscimento di stati fisici quali dolore od affaticamento.

- **Sistemi di IA ad alto rischio**
  Vi rientrano tutti quei sistemi che possono impattare in maniera significativa sulla vita delle persone.
  Il loro utilizzo è consentito ma solo in presenza di una serie di requisiti.
  In particolare, si tratta a titolo esemplificativo, di sistemi che rientrano in uno dei seguenti ambiti:
  - assunzione o selezione di persone fisiche, in particolare per pubblicare annunci di lavoro mirati, analisi o filtrazione di candidature e valutazione dei candidati;
  - adozione di decisioni riguardanti le condizioni dei rapporti di lavoro, la promozione o cessazione dei rapporti contrattuali di lavoro, assegnazione di compiti sulla base del comportamento individuale o dei tratti e delle caratteristiche personali;
  - monitoraggio e valutazione delle prestazioni e del comportamento delle persone nell'ambito di tali rapporti di lavoro.

- **Sistemi di IA a rischio limitato/minimo**
  Tali sistemi presentano un moderato rischio di impiego e sono soggetti ad obblighi di trasparenza, informando gli utilizzatori che stanno interagendo con sistemi di IA (es: chatbot come ChatGPT, software antispam).

3 Principi guida

3.1 Principi guida etici per l'IA

Le attività correlate alla trasformazione digitale ed all'utilizzo dell'IA devono basarsi sulla sistematica considerazione, ed applicazione, dei seguenti principi guida:

- L'utilizzo da parte della Società è inteso per migliorare le condizioni di lavoro e la produttività delle prestazioni lavorative nel pieno rispetto delle persone, dei loro diritti fondamentali e della sicurezza delle informazioni.
  Non può svolgersi in contrasto con la dignità umana, né può violare la riservatezza o la disponibilità dei dati personali o violare i principi di cybersecurity. Il trattamento dei dati dovrà avvenire sempre nel rispetto del disposto dal GDPR [3].
- L'accesso ai sistemi di IA deve garantire il rispetto dei principi di diversità, equità ed inclusione.
  La diversità include caratteristiche demografiche e personali quali, ad esempio: genere; identità di genere; età; disabilità; orientamento sessuale; etnia; nazionalità; razza; opinioni politiche o personali; credenze religiose.
- L'utilizzo dei sistemi di IA deve essere garantito senza recare pregiudizio a:
  - libertà di espressione ed associazione;
  - completezza, imparzialità e lealtà della comunicazione;
- Deve essere assicurata la cybersicurezza lungo l'intero ciclo di vita dei sistemi e dei modelli di IA, nel rispetto delle *policy* del Gruppo Tecniplast e delle leggi e normative applicabili.
  In particolare, deve essere assicurata la resilienza contro tentativi illeciti di modificare il loro utilizzo, comportamento e caratteristiche di sicurezza.
- Devono essere monitorati gli input ed il comportamento dei sistemi di IA.
  Particolare attenzione va posta nella gestione degli aggiornamenti di sistema, in quanto potrebbero influenzare il comportamento dei modelli di IA.
- La Società deve garantire il trattamento lecito, corretto e trasparente dei dati personali e la compatibilità con le finalità per le quali sono stati raccolti.
  La relativa informativa deve essere opportunamente comunicata o messa a disposizione degli interessati.

3.2 Linee guida per l'utilizzo dell'IA

In aggiunta ai sopraccitati principi guida etici ed al fine di un utilizzo corretto dell'IA nelle attività di business, sono stabilite le seguenti linee guida:

- Utilizzare solamente le versioni aziendali dei chatbot (Copilot, Chat GPT, etc): le versioni gratuite non danno alcuna garanzia di sicurezza e non diffusione di

informazioni, con conseguenze potenzialmente molto pericolose in termini di business e legali.

- Essere specifici nelle richieste e nell'interazione con l'IA: richieste generiche o approssimative generano risultati generici o approssimativi. Fornire sempre un contesto di riferimento e date istruzioni precise sulle aspettative (es: stile di scrittura, lunghezza del contenuto, cosa includere e cosa escludere, livello di dettaglio).
- Evitare di fornire informazioni ridondanti o non pertinenti alla richiesta: informazioni inutili generano "rumore di fondo" e defocalizzano l'IA.
- Esaminare sempre, e criticamente, i risultati: l'IA non ragiona come un essere umano, ed è suscettibile ad allucinazioni o conclusioni errate se non correttamente guidata. La supervisione umana sui risultati (*Human-In-The-Loop*) è irrinunciabile.

3.3 Principi guida tecnici

In coerenza con la definizione di trasformazione digitale e ad integrazione dei sopraccitati principi guida etici, le iniziative di trasformazione digitale eligibili devono soddisfare i seguenti principi guida tecnici:

1. Il numero di attori e di passi in un processo deve essere ridotto allo stretto indispensabile, e deve escludere attività che non generano oggettivo valore.
2. Compiti omogenei devono essere svolti con processi omogenei.
3. Per ogni processo, un'informazione inserita manualmente deve essere inserita una, ed una sola, volta.
4. Le informazioni inserite manualmente devono essere limitate allo stretto indispensabile.
5. Non sono ammesse attività manuali che possano essere svolte automaticamente od in modo digitale, salvo che l'esecuzione manuale sia economicamente più conveniente.
6. Per ogni informazione od elemento di processo esite una –ed una sola- fonte di origine (master).
7. Tutte le fonti derivate (slave) vengono alimentate dalle fonti master interessate.
8. Attività omogenee devono essere svolte con sistemi omogenei.
9. Le strutture dati di non esclusivo uso da parte di un processo, o sistema, devono essere condivise e riconducibili alla medesima struttura logica.
10. Non sono ammessi sistemi che limitino l'interscambio dati. La facilità di interscambio dati è un requisito discriminante.

Come regola generale:

- le iniziative che soddisfano tutti e dieci principi guida sono considerate "eligibili";
- le iniziative che soddisfano meno di otto principi guida sono considerate "non eligibili";
- le iniziative che soddisfano otto o nove principi guida devono essere esaminate per essere considerate "eligibili" o "non eligibili".

Le iniziative eligibili sono quindi ulteriormente valutate in termini di similarità, dipendenze e costi/benefici al fine di costruire la Roadmap di trasformazione digitale.
Essa viene rivalutata ogni anno, o quando la situazione lo richiede.

I sopraccitati principi guida tecnici materializzano la logica secondo la quale una iniziativa di trasformazione digitale eligibile deve essere affrontata considerando in cascata:

- L'ottimizzazione dei processi interessati;
- la predisposizione e l'affinamento dei dati e delle informazioni necessari al loro corretto funzionamento;
- le architetture informatiche e gli applicativi software utilizzati per la gestione dei sopraccitati processi.

4 Sistema di gestione dell'IA

Al fine di assicurare uno sviluppo, uso e gestione responsabile e sicura dei sistemi di IA nel rispetto dei principi guida enunciati nella presente policy, la Società deve adottare le sottoelencate prassi.

4.1 Sorveglianza

- La Società deve istituire opportuni meccanismi di sorveglianza sui sistemi di IA adottati, assicurando la possibilità di intervento umano (Human-In-The-Loop), nonché che il sistema di IA rispetti le vigenti leggi in materia.
- Il personale incaricato della sorveglianza deve possedere le necessarie competenze, nonché adeguata formazione ed autorità.
- In particolare per i sistemi di IA ad alto rischio, la Società dovrà effettuare una valutazione preventiva prima di autorizzarne il relativo utilizzo.

4.2 Misure tecniche ed organizzative

A prescindere dalla classe del rischio dei sistemi IA, la Società deve provvedere a:

- effettuare una valutazione del rischio identificando i potenziali rischi e danni associati all'utilizzo dei sistemi di AI nonché la probabilità e l'impatto degli stessi, (ad esempio: rischi di distorsione dei dati utilizzati per l'addestramento (*data poisoning*), o dall'uso di componenti pre-addestrati utilizzati per l'addestramento dei modelli (*model poisoning*);
- implementare standard di sicurezza (protezione da violazioni, perdite ecc.) e trasparenza (comprensibilità e documentazione chiara dei modelli IA, in ottemperanza ai principi di *accountability* del GDPR [3]);
- verificare la conformità del trattamento a quanto disposto dal GDPR [3];
- rafforzare le misure di sicurezza per proteggere i sistemi di IA da attacchi informatici e violazioni dei dati, laddove possibile ed applicabile;
- garantire che gli algoritmi di IA siano privi di pregiudizi e non creino discriminazioni, adottando pratiche di verifica e revisione;
- stabilire meccanismi per un efficace supervisione umana dei sistemi di IA;
- formare il personale interessato all'utilizzo responsabile dei sistemi di IA ed al rispetto dei diritti dei lavoratori;
- mantenere una documentazione dettagliata dei sistemi di IA utilizzati e delle procedure di valutazione del rischio.

Nello specifico caso di sistemi IA ad alto rischio, la Società deve inoltre:

- adottare misure tecniche ed organizzative adeguate ad un utilizzo conforme, assicurandosi che tali sistemi soddisfino i requisiti di sicurezza e trasparenza.
- affidare la sorveglianza umana e l'utilizzo dei sistemi di AI a persone competenti;
- monitorare il funzionamento dei sistemi;
- effettuare una valutazione d'impatto sui diritti fondamentali ex art. 27 dell'AI Act [2].

4.3 Formazione, informativa, *whistleblowing*

- La Società deve impartire al personale interessato ed agli utilizzatori un adeguato livello di formazione affinché possano comprendere appieno e valutare i potenziali rischi associati ai sistemi che utilizzano, comportandosi di conseguenza;
- nell'uso dei sistemi di IA, devono essere chiaramente identificati come generati artificialmente tutti i contenuti grafici, video e audio generati da sistemi di IA che plausibilmente assomigliano a persone, cose o luoghi esistenti (*Deep Fake*).

  Ciò anche al fine di preservare il rispetto del principio di trasparenza e della normativa in materia di *copyright*;
- la Società deve adeguatamente tutelare i segnalanti di azioni o prassi contrarie alla presente *policy*, in ottemperanza a quanto previsto dalla Società e dalle leggi applicabili in materia di *whistleblowing*.

5 Requisiti dei *provider* di IA

Nella scelta dei fornitori di sistemi e modelli di IA devono essere privilegiate le soluzioni che garantiscono la localizzazione e l'elaborazione dai dati presso data center dotati di robuste procedure di *disaster recovery* e *business continuity*, ed in grado di assicurare i più elevati standard in termini di sicurezza e trasparenza nelle modalità di sviluppo ed addestramento di applicazioni basate su IA generativa.

In particolare, ai fornitori interessati è richiesto di:

- garantire il rispetto di tutte le obbligazioni previste nell' AI Act [2] e nelle altre norme europee di riferimento, nonché delle disposizioni contenute nella presente *policy*, per quanto di loro competenza;
- assicurare la trasparenza di funzionamento dei sistemi di IA (come operano, le loro capacità e limitazioni), e fornire l'informativa necessaria affinché la presa di decisioni basate su di essi avvenga in modo consapevole;
- notificare se quello fornito può essere considerato un sistema di IA e quale ne è il livello di rischio;
- adottare misure di sicurezza che tengano in debito conto:
  - complessità dei modelli di IA (architettura e numerosità dei parametri);
  - congruenza dei modelli col loro utilizzo;
  - capacità di interpretare e spiegare gli output ottenuti;
  - caratteristiche del dataset di addestramento (dimensione, integrità, qualità, sensitività, attualità, rilevanza, diversità);
  - rilevanza nell'utilizzo di tecniche di irrobustimento dei modelli (es: *adversarial training*).

6 Meccanismi attuativi e di controllo

Il rispetto della presente *policy* viene verificato attraverso:

- istituzione di organismi di indirizzo e sorveglianza;
- *audit* interni da parte di organismi incaricati dalla Società.

La Società redige procedure ed istruzioni operative atte all'applicazione della presente *policy* ed alla verifica della sua efficacia.
Misure dell'efficacia possono essere ad esempio statistiche relative a:

- diffusione interna ed esterna;
- grado di comprensione della *policy*;
- numerosità degli audit e loro risultanze;
- casi segnalati di infrazione della *policy*.

7 Comportamenti

7.1 Comportamenti attesi

Con riferimento ai sopraccitati principi guida ed a prescindere dal tipo di attività svolto, sono attesi i seguenti comportamenti:

- ogni Dipendente della Società, a prescindere dal ruolo o dall'inquadramento, ha il dovere di comportarsi -nella forma e nei fatti- secondo i principi contenuti nella presente *policy*;
- ogni responsabile della gestione di collaboratori ha il dovere di vigilare sulla applicazione dei principi contenuti nella presente *policy*, agendo opportunamente in caso di situazioni critiche;
- ogni *provider* di IA ha il dovere di adempiere a quanto richiesto dalla presente *policy*, per quanto di sua competenza.

7.2 Comportamenti sanzionabili

Sono considerati comportamenti sanzionabili:

- l'infrazione, da parte di chiunque dei principi contenuti nella presente policy;
- la non vigilanza, da parte del personale incaricato in materia dalla Società, sul rispetto della presente policy;
- l'infrazione, da parte dei provider di IA, dei principi ad essi applicabili enunciati nel Codice di Condotta [1] e nella presente policy;
- la non applicazione, o l'inesatta applicazione, della presente policy.

Nel caso di comportamenti sanzionabili posti in essere da parte dei destinatari della presente *policy*, la Società si riserva il diritto di procedere al loro sanzionamento in modo commisurato alla loro gravità ed ai conseguenti effetti conclamati o potenziali, e sempre nel rispetto delle vigenti leggi e regolamenti in materia giuslavoristica.

Nel caso di comportamenti sanzionabili posti in essere da parte dei *provider* di IA si applicano i rimedi previsti dalla legge, nonché le disposizioni che regolano il rapporto di fornitura.

FINE DEL DOCUMENTO

(pagina intenzionalmente vuota)