POLICY PER L'UTILIZZO DELL'INTELLIGENZA ARTIFICIALE IN CITTÀ METROPOLITANA DI GENOVA

Versione: 3.0
Data: 23 Gennaio 2026

Tabella di Gestione del Documento

Vers	Data	Autore/i	Descrizione delle Modifiche	Stato	Approvato da
1.0	10/09/25	L. Papaleo (RTD)	Prima stesura della policy: definizione principi, governance iniziale e linee guida operative.	Superato	N/A
1.1	**16/09/25**	L. Papaleo (RTD)	Raffinamento contenuti su principi e linee guida operative AI Generativa.	superato	*N/A*
2.0	**17/09/25**	L. Papaleo (RTD), F. Rossi	**Revisione:** Integrazione fonti AgID e framework normativi. Istituzione del GL-IA e approccio basato sul rischio Dettaglio regole IA Generativa	Bozza da discutere con DG	*N/A*
3.0	**23/01/26**	L. Papaleo (RTD), M. Mordacci (DG)	**Revisione:** Aggiornamento sezione governance e correzioni minime su riferimenti e sezioni generali	Versione finale	*Con Decreto Sindaca Matropolitana n.__ del __/__/____*

SOMMARIO

Premessa e Finalità 3

Articolo I. **Ambito di Applicazione** 3

Articolo II. **Principi Fondamentali** 3

Articolo III. **Governance e Ruoli** 4

Articolo IV. **Ciclo di Vita dei Sistemi di IA** 6

Articolo V. **Linee Guida per l'Uso della IA Generativa** 7

Articolo VI. **Formazione e Cultura dell'Innovazione** 7

Articolo VII. **Trasparenza verso i Cittadini** 8

Articolo VIII. **Tutela della Proprietà Intellettuale** 8

Articolo IX. **Inosservanza della Policy** 8

Articolo X. **Riferimenti Normativi e Strategici** 9

Articolo XI. **Revisione della Policy** 10

Allegato A **Glossario** 11

PREMESSA E FINALITÀ

La Città Metropolitana di Genova riconosce il potenziale dell'Intelligenza Artificiale (IA) come strumento strategico per migliorare l'efficienza dei servizi pubblici, ottimizzare i processi decisionali e promuovere lo sviluppo sostenibile del territorio.

Questa policy ha l'obiettivo di definire un quadro di riferimento etico e operativo per l'introduzione e l'utilizzo di sistemi di IA all'interno dell'Ente, garantendo che ogni applicazione sia sviluppata e impiegata nel pieno rispetto dei diritti fondamentali dei cittadini, dei principi di trasparenza, equità e responsabilità, e in piena coerenza con il nuovo quadro normativo europeo sull'IA (Regolamento (UE) 2024/1689, "AI Act").

L'approccio dell'Ente è orientato alla **sperimentazione responsabile** e all'adozione graduale di soluzioni di IA, con una costante supervisione umana e un'attenzione prioritaria alla sicurezza dei dati e alla centralità della persona.

La presente Policy è coordinata con gli strumenti di programmazione dell'Ente (DUP, PIAO, Piano Strategico, Piano Triennale ICT - quando adottato) e ne costituisce riferimento operativo per la pianificazione, l'acquisizione e la gestione di sistemi di IA.

Articolo I. AMBITO DI APPLICAZIONE

La presente policy si applica a tutte le fasi del ciclo di vita (progettazione, sviluppo, acquisizione, formazione, utilizzo, monitoraggio e dismissione) di qualsiasi sistema di IA impiegato dall'Ente.

È vincolante per **tutto il personale dipendente, i dirigenti e i collaboratori esterni** che, a qualsiasi titolo, partecipano all'implementazione o all'utilizzo di tali sistemi.

La Policy si applica anche ai fornitori e partner che progettano, forniscono o gestiscono per conto dell'Ente componenti o servizi di IA. Tali soggetti devono conformarsi alle presenti disposizioni e alle clausole contrattuali dedicate.

Articolo II. PRINCIPI FONDAMENTALI

Ogni iniziativa legata all'IA deve inderogabilmente attenersi ai seguenti principi:

(1) Antropocentrismo e Supervisione Umana (Human-in-the-Loop): Ogni sistema automatico deve prevedere la **supervisione umana qualificata**, specialmente nei processi che hanno un impatto sui diritti e gli interessi dei cittadini. Nessuna decisione con effetti legali o significativi può essere completamente automatizzata.

(2) Equità e Non Discriminazione: L'Ente si impegna a prevenire e mitigare la creazione o l'amplificazione di bias. Le basi di dati utilizzate devono essere verificate per garantirne la **qualità, la correttezza, la completezza e la rappresentatività**.

(3) Trasparenza e Spiegabilità (XAI): I processi decisionali guidati dall'IA devono essere **comprensibili e tracciabili**. Deve essere possibile spiegare la logica di funzionamento e le ragioni di un risultato, come richiesto dal diritto alla spiegazione.

(4) Sicurezza e Protezione dei Dati (Privacy by Design/Default): Ogni soluzione di IA deve essere progettata nel rigoroso rispetto del GDPR, minimizzando i dati trattati e adottando le più adeguate misure di sicurezza informatica.

(5) Responsabilità e Rendicontazione (Accountability): Deve essere sempre chiaramente identificato un Responsabile del Sistema IA per ogni applicazione in uso, che ne risponda in termini di funzionamento, impatto e conformità.

(6) Sostenibilità: L'utilizzo degli strumenti di IA deve tenere conto del loro impatto ambientale e sociale. L'Ente promuove un approccio consapevole che ottimizzi l'uso delle risorse computazionali, privilegiando, ove possibile, soluzioni a minore consumo energetico.

(7) Proporzionalità e Minimizzazione del Rischio: la complessità delle soluzioni IA deve essere proporzionata alla finalità pubblica perseguita; si privilegiano soluzioni meno intrusive e più interpretabili a parità di risultato.

(8) Auditabilità e Tracciabilità: per ciascun sistema IA devono essere definiti registri/log di funzionamento e decisione adeguati allo scopo, conservati secondo le norme archivistiche.

(9) Contestabilità: ogni decisione automatizzata o assistita dall'IA deve poter essere compresa, riesaminata e, se del caso, corretta da un operatore umano entro termini ragionevoli.

Articolo III. GOVERNANCE E RUOLI

Assetto di governance dell'Intelligenza Artificiale: La governance dei sistemi di Intelligenza Artificiale della Città Metropolitana di Genova è affidata a un presidio centrale unitario, finalizzato a garantire responsabilità, coerenza strategica e conformità normativa nell'adozione e nell'uso dell'IA. La governance è esercitata congiuntamente da: il Direttore Generale e Segretario Generale; il Responsabile per la Transizione Digitale (RTD) con il supporto dell'Ufficio per la Transizione Digitale (UTD). Il presidio centrale di governance:

- assicura la coerenza dell'uso dell'IA con gli strumenti di programmazione dell'Ente (DUP, PIAO, Piano Strategico, Piano Triennale ICT – quando adottato);
- garantisce il rispetto del quadro normativo vigente (AI Act, normativa nazionale, GDPR, CAD, Linee guida AgID);
- supervisiona l'attuazione della presente Policy lungo l'intero ciclo di vita dei sistemi di IA.

Ruolo del RTD e dell'Ufficio per la Transizione Digitale: Il RTD, avvalendosi dell'UTD:

- coordina operativamente l'attuazione della presente Policy;
- supporta le Direzioni e i Servizi nella progettazione, acquisizione, utilizzo e dismissione dei sistemi di IA;
- cura l'istituzione e la pubblicazione del Registro Pubblico delle IA (in cui aggiornamento dei contenuti è responsabilità delle Direzioni tecniche coinvolte);

- promuove l'adozione di standard, modelli e checklist di conformità, in coerenza con l'approccio basato sul rischio;
- assicura il raccordo con i profili di sicurezza informatica, architettura ICT e interoperabilità.

Collaborazioni operative e competenze specialistiche: Per ciascun sistema di IA o caso d'uso, il presidio centrale di governance attiva collaborazioni operative mirate, in funzione delle caratteristiche del sistema, della finalità perseguita e dei rischi connessi. Sono obbligatoriamente coinvolti:

- il Responsabile della Protezione dei Dati (DPO), nei casi in cui il sistema comporti trattamenti di dati personali o rischi per i diritti e le libertà degli interessati, inclusa l'eventuale DPIA;
- il Responsabile della Stazione Unica Appaltante e/o il RUP, in caso di acquisizione o affidamento di sistemi o servizi di IA;
- le strutture ICT competenti, per gli aspetti di sicurezza, architettura, integrazione e continuità operativa.

Possono inoltre essere coinvolti, in relazione allo specifico ambito di applicazione, i Direttori delle Direzioni tecniche, il Responsabile delle Risorse Umane, le strutture competenti in materia di trasparenza, anticorruzione, controlli interni, nonché ulteriori competenze specialistiche. Le collaborazioni hanno natura operativa e contestualizzata e non comportano l'istituzione di organismi permanenti ulteriori.

Responsabile del Sistema IA: Per ciascun sistema di Intelligenza Artificiale adottato o utilizzato dall'Ente è individuato un Responsabile del Sistema IA, quale punto di riferimento unico per la responsabilità amministrativa dell'uso del sistema. Il Responsabile del Sistema IA coincide, di norma:

- con il Direttore/Dirigente responsabile del settore o del servizio nell'ambito del quale il sistema è utilizzato;
- con il Direttore Generale, nei casi in cui il sistema di IA abbia carattere trasversale, incida su più strutture organizzative o supporti funzioni di coordinamento generale dell'Ente.

Il Responsabile del Sistema IA:

- garantisce che il sistema sia utilizzato esclusivamente per le finalità istituzionali previste;
- assicura il rispetto dei principi di supervisione umana, trasparenza, proporzionalità e non discriminazione;
- vigila sull'attuazione delle eventuali misure di mitigazione dei rischi definite in sede di istruttoria;
- collabora con RTD e UTD per il monitoraggio del sistema, la gestione degli incidenti e l'aggiornamento del Registro Pubblico delle IA;
- garantisce, ove applicabile, la possibilità di contestazione e riesame delle decisioni assistite dall'IA.

Il Responsabile del Sistema IA non coincide con il fornitore del sistema, né con il DPO o con il RUP, che operano secondo i rispettivi ruoli e responsabilità previsti dalla normativa vigente.

Responsabilità dei Direttori e dei Dirigenti: I Direttori e i Dirigenti restano responsabili dei procedimenti e dei servizi di competenza in cui sono utilizzati sistemi di IA e garantiscono:

- la corretta istruttoria delle proposte di adozione o utilizzo dei sistemi;
- la collaborazione con il presidio di governance, il RTD e l'UTD;
- l'applicazione delle misure di supervisione umana e di mitigazione dei rischi;
- le attività di monitoraggio e segnalazione previste dalla presente Policy.

Articolo IV. Ciclo di Vita dei Sistemi di IA

FASE 1 Progettazione e Acquisizione: Prima di avviare un progetto o acquistare una soluzione di IA, è obbligatoria una **valutazione preliminare** che includa:

- **Classificazione del rischio** del sistema (inaccettabile, alto, limitato, minimo). I sistemi a rischio inaccettabile sono vietati.
- Analisi dei benefici pubblici e dell'effettiva necessità.
- Verifica della qualità e della liceità delle fonti dati.
- La conformità ai principi dell'Art. II.
- Richiesta ai fornitori di documentazione completa su funzionamento, limiti e requisiti di trasparenza del sistema. Il fornitore deve rendere disponibili almeno: (a) Model Card del sistema, (b) Datasheet dei dataset utilizzati/previsti, (c) metriche di prestazione (accuratezza, robustezza, tassi di errore e loro impatto), (d) limitazioni note e casi d'uso vietati, (e) requisiti di explainability e logging, (f) piano di monitoraggio post-messa in esercizio e gestione delle versioni.

Priorità a Strumenti Qualificati: Nella scelta di soluzioni IA basate su cloud, deve essere data priorità a software e servizi qualificati e presenti nel Catalogo dei servizi cloud dell'Agenzia per la Cybersicurezza Nazionale (ACN), o che comunque offrano garanzie equivalenti in termini di sicurezza e conformità normativa. I servizi cloud devono essere qualificati ai sensi del Catalogo ACN o garantire misure equivalenti (sicurezza, localizzazione/trasferimenti, continuità operativa), documentate in sede di gara/contratto.

FASE 2 Sviluppo e Validazione: Ogni sistema deve essere testato in un ambiente controllato prima del rilascio, per verificarne l'affidabilità, la robustezza e l'assenza di bias discriminatori.

È suggerita una checklist di conformità pre-messa in esercizio che includa: esito classificazione rischio AI Act; esito VIA/DPIA ove dovute; test di robustezza/bias; piano di supervisione umana; piano di dismissione; configurazione logging; esito pen-test/cyber ove pertinente.

FASE 3 Monitoraggio e Dismissione: I sistemi di IA in esercizio sono soggetti a monitoraggio continuo per garantirne il corretto funzionamento nel tempo. La loro dismissione deve essere pianificata e gestita in sicurezza. Devono essere definiti KPI e soglie di allerta. Superate le soglie, si attiva l'Incident Reporting IA al GL-IA. In dismissione, si prevede: bonifica/smaltimento sicuro dei dati e dei modelli, conservazione degli atti/decisioni secondo norme archivistiche, comunicazione al Registro Pubblico.

Articolo V. LINEE GUIDA PER L'USO DELLA IA GENERATIVA

In attesa della definizione di un elenco ufficiale di strumenti autorizzati, il personale può utilizzare strumenti di IA generativa disponibili sul mercato **solo per attività a basso rischio** (es. supporto alla scrittura di bozze, schemi di presentazioni, riassunti non sensibili), nel pieno rispetto dei divieti di inserimento di dati personali, riservati o segreti d'ufficio.

L'uso di modelli linguistici e di IA generativa da parte del personale è consentito, quindi, come supporto all'attività lavorativa (es. per bozze, riassunti, brainstorming), a condizione che vengano rispettate le seguenti regole inderogabili:

Divieto Assoluto di Inserire Dati Sensibili: È vietato inserire in strumenti di IA generativa (specialmente se basati su cloud pubblico) dati personali, informazioni riservate, segreti d'ufficio o qualsiasi dato non di dominio pubblico.

Obbligo di Verifica Critica e Responsabilità: L'output generato da un'IA **non è mai da considerarsi una fonte autorevole**. L'operatore umano che lo utilizza è **sempre e completamente responsabile** del risultato finale. È obbligatorio:

- Verificare l'accuratezza, la veridicità e la coerenza delle informazioni prodotte.
- Rielaborare profondamente i testi per garantirne l'originalità e l'adeguatezza allo stile della Pubblica Amministrazione.

Trasparenza: Non è consentito utilizzare "copia-incolla" da IA generative per la redazione di atti amministrativi o documenti ufficiali. L'IA può essere usata per la ricerca, l'ideazione o la stesura di bozze, ma il prodotto finale deve essere frutto del lavoro intellettuale del dipendente.

Uso in Front-Office: Laddove l'IAG venga impiegata in servizi rivolti ai cittadini (es. chatbot), devono essere garantiti: (i) etichettatura chiara della natura non umana dell'interlocutore, (ii) canale alternativo umano sempre disponibile, (iii) registrazione e conservazione delle conversazioni secondo normativa, (iv) prevenzione di impersonation/deepfake, (v) filtri su contenuti inappropriati.

Usi vietati: Sono vietati: generazione di contenuti fuorvianti o manipolativi, simulazione di identità, elusione di norme/procedure, redazione automatica di atti amministrativi senza piena stesura/assunzione di responsabilità da parte dell'operatore umano.

Responsabilità Personale dell'Utente: Fermo restando il ruolo del Responsabile del Sistema IA, ogni dipendente che utilizza strumenti di IA, in particolare generativa, è personalmente responsabile delle implicazioni etiche e giuridiche delle proprie azioni e dei contenuti prodotti. La supervisione umana e la verifica critica dei risultati sono un dovere inderogabile.

Articolo VI. FORMAZIONE E CULTURA DELL'INNOVAZIONE

La Città Metropolitana di Genova si impegna a promuovere un programma di formazione continua per diffondere tra il personale le competenze necessarie a comprendere e utilizzare consapevolmente gli

strumenti di IA, riconoscendone le opportunità e i limiti. La partecipazione alle iniziative formative fondamentali individuate dall'Ente costituisce un dovere per il personale interessato.

La formazione è organizzata su tre livelli: (1) Base per tutto il personale (fondamenti IA, rischi, regole IAG), (2) Avanzata per dirigenti e RUP/RESP. di procedimento (governance del rischio, responsabilità, procurement), (3) Specialistica per Servizio ICT/GL-IA/DPO (tecnica, sicurezza, VIA/DPIA, explainability). I moduli sono aggiornati almeno annualmente e inseriti nel Piano della Formazione e nel PIAO.

Articolo VII. Trasparenza verso i Cittadini

L'Ente pubblicherà sul proprio sito istituzionale un registro delle soluzioni di IA (Registro Pubblico delle IA) utilizzate che hanno un impatto sui servizi al cittadino. Per ogni soluzione, verranno indicate in modo semplice e chiaro:

- La finalità del sistema.
- La logica di funzionamento di base.
- Il responsabile del procedimento.

Il Registro Pubblico delle IA è aggiornato almeno annualmente ed è pubblicato anche come open data. Per ogni sistema sono indicati: finalità; basi normative; livello di rischio; presenza di supervisione umana; principali metriche/limitazioni; contatti per chiarimenti; canale di reclamo/contestazione e tempi di risposta.

Il canale di reclamo/contestazione è gestito in coordinamento con l'Ufficio dell'ente preposto ai reclami e segue le procedure standard dell'Ente per la gestione delle segnalazioni, garantendo tempi di risposta certi.

Articolo VIII. Tutela della Proprietà Intellettuale

È fatto obbligo di assicurarsi che i dati inseriti nei sistemi di IA e i contenuti da essi generati non violino i diritti d'autore o di proprietà intellettuale di terzi.

È vietato l'uso non autorizzato di contenuti protetti da diritto d'autore (copyright) come input per i sistemi. L'utente è responsabile di garantire che i materiali generati siano originali e non costituiscano plagio o violazione di opere esistenti.

I contratti con i fornitori devono prevedere manleva per violazioni di diritti di terzi connesse a modelli/dataset, e garanzie su licenze d'uso degli output generati. È vietato l'uso di dataset/addestramenti privi di lecita provenienza o di idonee licenze.

Articolo IX. Inosservanza della Policy

La violazione delle disposizioni contenute nella presente policy, in base alla gravità, potrà comportare l'applicazione delle sanzioni disciplinari previste dalla normativa vigente e dai regolamenti interni dell'Ente, fatto salvo l'eventuale rilievo in sede civile, penale o erariale. È tutelata la segnalazione in buona fede (whistleblowing) di usi impropri.

Articolo X. RIFERIMENTI NORMATIVI E STRATEGICI

La presente Policy è redatta in coerenza e conformità con i principali quadri di riferimento europei, nazionali e internazionali in materia di intelligenza artificiale, innovazione digitale, organizzazione amministrativa e protezione dei dati personali. In particolare, si richiamano i seguenti atti e documenti di riferimento:

- Regolamento (UE) 2024/1689 del Parlamento europeo e del Consiglio – "AI Act", che stabilisce regole armonizzate sull'intelligenza artificiale e introduce un approccio basato sul rischio, definendo obblighi per fornitori e utilizzatori di sistemi di IA. Testo ufficiale in lingua italiana (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2024/1689/oj?locale=it
- Regolamento (UE) 2016/679 – Regolamento Generale sulla Protezione dei Dati (GDPR), che costituisce il riferimento fondamentale per il trattamento lecito, corretto e trasparente dei dati personali, inclusi quelli utilizzati nei sistemi di IA. Testo ufficiale (EUR-Lex): https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=it
- Legge n. 132 del 23 settembre 2025 – "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", entrata in vigore il 10 ottobre 2025, che definisce principi, criteri e interventi settoriali relativi all'utilizzo dei sistemi di IA nel contesto italiano, in coerenza con il Regolamento UE 2024/1689. Testo (Normattiva): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2025-09-23;132!vig=2025-10-10
- Codice dell'Amministrazione Digitale – Decreto Legislativo 7 marzo 2005, n. 82 e s.m.i., che disciplina l'uso delle tecnologie digitali nella Pubblica Amministrazione, promuovendo efficienza, trasparenza e qualità dei servizi. Testo vigente (Normattiva): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2005-03-07;82
- Linee Guida AgID per l'adozione di sistemi di Intelligenza Artificiale nella Pubblica Amministrazione, che forniscono indirizzi tecnici e organizzativi per un utilizzo responsabile e conforme dell'IA nel settore pubblico. Portale ufficiale AgID – sezione IA: https://www.agid.gov.it/it/ambiti-intervento/intelligenza-artificiale
- Strategia Italiana per l'Intelligenza Artificiale, quale documento di indirizzo strategico del Governo italiano per lo sviluppo e l'adozione dell'IA secondo un approccio antropocentrico, affidabile e sostenibile. Documento ufficiale (AgID / Dipartimento per la trasformazione digitale): https://www.agid.gov.it/it/agenzia/stampa-e-comunicazione/notizie/2024/07/22/pubblicato-il-documento-completo-strategia-italiana-lintelligenza-artificiale-2024
- Testo Unico delle Leggi sull'Ordinamento degli Enti Locali (TUEL) – Decreto Legislativo 18 agosto 2000, n. 267, con riferimento ai principi di organizzazione, responsabilità dirigenziale e ruolo degli organi apicali dell'Ente. Testo vigente (Normattiva): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2000-08-18;267
- Piano Integrato di Attività e Organizzazione (PIAO), di cui al Decreto-Legge 9 giugno 2021, n. 80, convertito con modificazioni dalla Legge 6 agosto 2021, n. 113, quale strumento di coordinamento tra organizzazione, performance, gestione del rischio, trasparenza e sviluppo delle competenze. Testo (Normattiva): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legge:2021-06-09;80

- Codice dei contratti pubblici – Decreto Legislativo 31 marzo 2023, n. 36, per gli aspetti relativi all'acquisizione di sistemi e servizi di IA e alla disciplina dei rapporti con i fornitori. Testo vigente (Normattiva): https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2023-03-31;36
- Orientamenti etici per un'Intelligenza Artificiale affidabile (Commissione Europea, Gruppo di esperti ad alto livello sull'IA, 2019), quali riferimenti etici e valoriali per lo sviluppo e l'uso di sistemi di IA rispettosi dei diritti fondamentali. Documento ufficiale: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai
- Principi dell'OCSE sull'Intelligenza Artificiale – Raccomandazione del Consiglio dell'OCSE (2019), quali principi di riferimento internazionale per un'IA innovativa, affidabile e orientata allo sviluppo sostenibile. Documento ufficiale: https://www.oecd.org/sti/ieconomy/principi-ocse-sull-intelligenza-artificiale.htm

Articolo XI. Revisione della Policy

La presente policy è un documento dinamico. Verrà riesaminata e, se necessario, aggiornata con cadenza annuale o per allinearla alle progressive scadenze di applicazione previste dal quadro normativo, con particolare riferimento all'AI Act europeo.

Il Direttore e Segretario Generale propone le modifiche in coordinamento con il RTD. L'atto di aggiornamento sostanziale è approvato con le stesse modalità dell'adozione iniziale. È mantenuto un Change Log (versioni, data, modifiche principali).

ALLEGATO A GLOSSARIO

Di seguito sono riportate le definizioni dei principali termini utilizzati nella presente policy, al fine di garantirne una comprensione uniforme.

Algoritmo: Una sequenza finita di istruzioni o regole logico-matematiche che viene eseguita da un computer per risolvere un problema o svolgere un compito specifico. È il "motore" di un sistema di IA.

Anonimizzazione: Processo che modifica i dati personali in modo irreversibile, così da rendere impossibile identificare la persona a cui si riferiscono.

Bias (Distorsione): Una tendenza sistematica di un algoritmo a produrre risultati che favoriscono o sfavoriscono ingiustamente determinati gruppi o individui. Il bias può derivare da dati di addestramento incompleti, errati o non rappresentativi della realtà.

Ciclo di Vita dell'IA: L'insieme di tutte le fasi relative a un sistema di IA, dalla sua ideazione e progettazione iniziali, passando per lo sviluppo, l'addestramento (training), la validazione, l'implementazione (messa in esercizio), il monitoraggio continuo, fino alla sua dismissione finale.

DPIA: valutazione d'impatto sulla protezione dei dati ai sensi del GDPR.

Human-in-the-Loop (Supervisione Umana): Un modello di interazione in cui un essere umano è costantemente coinvolto nel processo decisionale di un sistema di IA. L'umano monitora, valida, corregge o annulla le decisioni dell'algoritmo, specialmente quelle più critiche, mantenendo il controllo finale.

Incident Reporting IA: procedura di segnalazione e gestione di eventi avversi o anomalie dei sistemi IA.

Intelligenza Artificiale (IA): Un sistema software progettato per eseguire compiti che normalmente richiederebbero l'intelligenza umana, come il ragionamento, l'apprendimento, la pianificazione e la comprensione del linguaggio. Ai sensi dell'AI Act, è *un sistema automatizzato che può, per una data serie di obiettivi, generare output come previsioni, contenuti, raccomandazioni o decisioni*.

Intelligenza Artificiale Generativa (IAG): Una branca dell'IA in cui i modelli sono in grado di creare contenuti nuovi e originali (testi, immagini, suoni) partendo da un input (prompt). Esempi noti sono ChatGPT, Gemini, Midjourney.

Model Card / Datasheet: documentazione standardizzata di modelli/dataset (scopo, prestazioni, limiti).

Modello di Fondazione: modello su larga scala impiegato come base per molteplici compiti (es. LLM).

Pseudonimizzazione: Processo che sostituisce i dati personali con identificatori artificiali (pseudonimi), rendendo possibile risalire all'identità della persona solo tramite informazioni aggiuntive conservate separatamente

Registro Pubblico delle IA: elenco pubblico dei sistemi IA dell'Ente con informazioni essenziali per i cittadini.

Sistema di IA ad Uso Generale (GPAI): sistema in grado di svolgere una varietà di compiti; può essere integrato in molteplici applicazioni.

Valutazione d'Impatto Algoritmico (VIA): Un processo di analisi preventiva finalizzato a identificare, valutare e mitigare i potenziali rischi e impatti negativi di un sistema di IA sui diritti fondamentali, l'equità, la sicurezza e la società prima della sua implementazione.

XAI (Explainable AI - Intelligenza Artificiale Spiegabile): Un insieme di metodi e tecniche che mirano a rendere comprensibile il processo decisionale di un sistema di IA, superando il problema della "scatola nera" (black box). La XAI permette di esporre la logica, i criteri e i dati che hanno portato l'algoritmo a un determinato risultato, garantendo trasparenza e accountability.