

POLICY IA FVGS

Sommario

PREMESSE.....	2
Art. 1 – Oggetto e finalità.....	2
Art. 2 – Ambito di applicazione.....	3
Art. 3 – Definizioni	3
Art. 4 – Principi inderogabili	4
Art. 5 – Governance, ruoli e responsabilità.....	6
Art. 6 – Registro e mappatura dei sistemi IA.....	7
Art. 7 – Classificazione del rischio e requisiti minimi.....	8
Art. 8 – Valutazioni di impatto e autorizzazione all'uso.....	9
Art. 9 – Monitoraggio, verifiche e misure di mitigazione	9
Art. 10 – Divieti.....	10
Art. 11 – Gestione fornitori e contratti	11
Art. 12 – Conservazione documentale	13
Art. 13 – Gestione dei dati personali nell'utilizzo dei sistemi di Intelligenza Artificiale.....	13
Art. 14 – Formazione	13
Art. 15 – Riesame e aggiornamento.....	14
Art. 16 – Entrata in vigore e diffusione	15

POLICY IA FVGS

PREMESSE

VISTO il Regolamento (UE) 2024/1689 (c.d. "AI Act") e la necessità di classificare e governare i **sistemi di Intelligenza Artificiale** (di seguito IA) in ragione del rischio;

VISTA la Legge 23 settembre 2025, n. 132, recante "Disposizioni e deleghe al Governo in materia di intelligenza artificiale", che stabilisce i principi nazionali per la ricerca, la sperimentazione, lo sviluppo, l'adozione e l'applicazione dei sistemi e dei modelli di intelligenza artificiale, in coordinamento con il Regolamento (UE) 2024/1689;

VISTO il Regolamento (UE) 2016/679 (GDPR), con particolare riferimento ai principi di liceità, correttezza, trasparenza, minimizzazione e alle garanzie in materia di decisioni automatizzate;

VISTI il Regolamento Privacy R 14.01 e il Regolamento Data Breach R 14.02 di FVGS vigenti;

VISTA la Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), in particolare gli articoli 4, in materia di controlli a distanza, 8, in materia di divieto di indagini sulle opinioni dei lavoratori e su fatti non rilevanti ai fini della valutazione dell'attitudine professionale, e 15, in materia di nullità degli atti discriminatori;

VISTA la Legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori), art. 4, in materia di controlli a distanza;

VISTO il D.Lgs. 8 giugno 2001, n. 231 e il Modello di Organizzazione, Gestione e Controllo (MOG) adottato da FVGS, con i relativi presidi di controllo interno;

VISTO il Regolamento per la gestione delle segnalazioni di illeciti (whistleblowing) e la tutela del segnalante (whistleblower) R 21.01 di FVGS vigente;

VISTI il D.Lgs. 19 agosto 2016, n. 175, il D.Lgs. 31 marzo 2023, n. 36 e il D.Lgs. 14 marzo 2013, n. 33;

CONSIDERATO che FVGS opera quale società a totale partecipazione pubblica soggetta a controllo analogo della Regione Autonoma Friuli Venezia Giulia e che l'adozione dell'IA deve avvenire nel rispetto di principi di accountability, tracciabilità e tutela dei diritti;

CONSIDERATO che l'IA può incidere su processi organizzativi, diritti dei lavoratori, protezione dei dati, salute e sicurezza, nonché su cybersicurezza e continuità operativa;

Tutto ciò premesso, FVGS adotta la presente Policy, quale atto interno vincolante per l'uso responsabile dell'IA.

Art. 1 – Oggetto e finalità

La presente Policy disciplina i principi, le responsabilità e i presidi organizzativi relativi all'adozione, all'utilizzo e al monitoraggio dei sistemi di IA all'interno di FVGS. La Policy ha natura di atto interno di indirizzo e governo e si propone di definire un quadro unitario di riferimento per l'impiego dell'IA nei processi aziendali, assicurando che tali tecnologie siano utilizzate quale strumento di supporto all'attività umana e decisionale e non quale sostituto della responsabilità delle persone e dell'organizzazione.

In particolare, la Policy persegue le seguenti finalità:

- garantire la conformità normativa europea e nazionale in materia di IA, protezione dei dati personali, lavoro e responsabilità dell'ente;
- assicurare un utilizzo dell'IA trasparente, controllato e proporzionato, fondato sulla supervisione umana e sulla tracciabilità dei processi;
- prevenire e mitigare rischi legali, organizzativi, reputazionali ed etici connessi all'impiego di sistemi di IA;

POLICY IA FVGS

- integrare l'adozione dell'IA nel sistema di governance e di controllo interno di FVGS, in coerenza con i presidi previsti dal MOG e dagli atti e regolamenti aziendali;
- promuovere un utilizzo dell'IA coerente con i principi di centralità della persona, tutela dei diritti fondamentali, dignità del lavoro e interesse pubblico.

La presente Policy costituisce pertanto il riferimento generale per l'adozione e l'utilizzo dei sistemi di IA in FVGS e si coordina con le ulteriori informazioni documentate aziendali applicabili.

Art. 2 – Ambito di applicazione

La presente Policy si applica a tutti i processi, le attività e i contesti organizzativi in cui siano adottati, utilizzati o comunque impiegati sistemi di IA, inclusi progetti pilota, sperimentazioni, prototipi e strumenti di IA a finalità generali, quando utilizzati per finalità lavorative o istituzionali.

La Policy trova applicazione con riferimento ai sistemi di IA rientranti nell'ambito di applicazione del *Regolamento (UE) 2024/1689 (AI Act)* e della *Legge 23 settembre 2025, n. 132*, indipendentemente dalla modalità di acquisizione, sviluppo o integrazione dei medesimi, nonché dalla loro collocazione infrastrutturale o tecnologica.

Le disposizioni della presente Policy sono vincolanti per tutti i soggetti che, a qualunque titolo, partecipano ai processi aziendali in cui l'IA è utilizzata, inclusi amministratori, dirigenti, dipendenti, collaboratori, consulenti, fornitori e partner tecnologici, nei limiti delle rispettive competenze e responsabilità.

La Policy si applica altresì ai sistemi di IA forniti o gestiti da soggetti terzi, qualora tali sistemi siano utilizzati nell'ambito delle attività di FVGS o incidano sui processi, sui lavoratori, sugli utenti o sui soggetti comunque interessati dall'azione aziendale.

Restano ferme le disposizioni più specifiche previste dalla normativa vigente, dagli atti e regolamenti aziendali applicabili, nonché dalle convenzioni e dagli accordi che disciplinano particolari ambiti di attività.

Art. 3 – Definizioni

Ai fini della presente Policy si applicano le definizioni di cui al Regolamento (UE) 2024/1689 (AI Act) e alla Legge 23 settembre 2025, n. 132. In particolare, si intende per:

- a) Sistema di Intelligenza Artificiale (Sistema di IA).** Un sistema automatizzato che elabora dati o input per generare output quali previsioni, raccomandazioni, classificazioni o supporti decisionali, con diversi livelli di autonomia, idonei a incidere su processi o attività aziendali.

Rientrano in tale definizione, a titolo esemplificativo:

- sistemi di supporto decisionale e di analisi;
- sistemi di classificazione, previsione o ottimizzazione;
- strumenti di automazione intelligente dei processi;
- funzionalità di IA integrate in software gestionali o applicativi aziendali.

- b) Modelli di Intelligenza Artificiale a finalità generali (GPAI).** Modelli di IA addestrati su grandi quantità di dati, capaci di svolgere una pluralità di compiti e di essere utilizzati in contesti diversi.

Rientrano in questa categoria, se impiegati per finalità lavorative:

- modelli di IA generativa (testo, immagini, codice, dati);
- assistenti digitali e strumenti generalisti di supporto ai contenuti.

POLICY IA FVGS

L'uso di GPAl in FVGS è ammesso esclusivamente come strumento di supporto, con supervisione umana.

- **IA ad alto rischio:** sistemi di IA che, secondo la classificazione dell'AI Act, possono incidere in modo significativo su diritti fondamentali, lavoro, sicurezza, salute o accesso a servizi essenziali. Tali sistemi sono soggetti a requisiti rafforzati di valutazione, documentazione, tracciabilità, supervisione umana e monitoraggio.
- **Decisione automatizzata:** una decisione o un esito prodotto da un sistema di IA senza un intervento umano significativo. Sono vietate le decisioni esclusivamente automatizzate con effetti giuridici o rilevanti sulle persone; la responsabilità finale resta sempre in capo a un soggetto umano.
- **Supervisione umana:** l'insieme delle misure che garantiscono la comprensione del funzionamento del sistema di IA, la possibilità di intervento sull'output e la responsabilità umana delle decisioni.
- **Utilizzatore:** qualsiasi soggetto interno o esterno a FVGS che utilizzi sistemi di IA nell'ambito di attività lavorative o processi aziendali.
- **Fornitore di sistemi di IA:** il soggetto che sviluppa, fornisce o integra sistemi di IA a favore di FVGS, anche tramite servizi o piattaforme di terze parti.
- **Dati:** qualsiasi informazione digitale, personale o non personale, utilizzata dai sistemi di IA, nel rispetto della normativa in materia di protezione dei dati e sicurezza delle informazioni.

Art. 4 – Principi inderogabili

FVGS adotta un approccio umano-centrico e prudentiale nell'uso dell'IA, assicurando che l'IA operi esclusivamente come strumento di supporto e non come sostituto del giudizio e della responsabilità umana.

I principi di cui al presente articolo costituiscono criteri interpretativi vincolanti per:

- l'applicazione della presente Policy;
- la valutazione della legittimità dell'uso dei sistemi di IA;
- l'attività di controllo dell'Organismo di Vigilanza, del RPCT e delle funzioni di audit.

L'adozione e l'utilizzo dei sistemi di IA in FVGS sono subordinati al rispetto dei seguenti principi inderogabili, che costituiscono presidi di prevenzione dei rischi legali e organizzativi.

L'utilizzo di sistemi di intelligenza artificiale a finalità generali (GPAl), inclusi strumenti di IA generativa, è consentito esclusivamente come supporto all'attività lavorativa, nel rispetto dei principi della presente Policy e delle istruzioni operative aziendali.

In particolare:

- è ammesso l'utilizzo per attività di supporto, quali redazione di bozze, sintesi, analisi preliminari e classificazione di informazioni;
- è vietato inserire nei sistemi di IA generativa:
 - dati personali non autorizzati;
 - dati sensibili o giudiziari;
 - informazioni riservate, strategiche o non pubbliche;
 - credenziali o dati di accesso ai sistemi aziendali;
- è fatto obbligo di verificare criticamente gli output generati e di non utilizzare tali sistemi come fonte autonoma di decisione.

L'output dei sistemi di IA generativa non ha valore autonomo e deve essere sempre validato da un soggetto umano, che ne mantiene la responsabilità.

a) Trasparenza, informazione e tracciabilità

POLICY IA FVGS

FVGS assicura che l'utilizzo di sistemi di IA sia:

- preventivamente dichiarato e documentato;
- tracciabile nelle sue finalità, modalità di utilizzo e ambiti applicativi;
- comprensibile per i soggetti coinvolti.

La documentazione dei sistemi di IA e delle decisioni supportate dagli stessi costituisce presidio essenziale di accountability e base informativa per i controlli interni.

b) Supervisione umana e responsabilità individuale

Ogni sistema di IA è utilizzato sotto la supervisione di un soggetto umano individuato, che:

- valuta criticamente gli output del sistema;
- può intervenire, correggere o annullare gli esiti prodotti;
- assume la responsabilità finale delle decisioni.

La responsabilità delle decisioni non è in alcun caso delegabile al sistema di IA. Sono vietate decisioni esclusivamente automatizzate con effetti giuridici o rilevanti sulle persone. **Equità, non discriminazione e prevenzione dei bias.**

FVGS adotta misure organizzative e di controllo volte a prevenire effetti discriminatori o distorsivi derivanti dall'uso dell'IA, con particolare riferimento a:

- bias nei dati, nei modelli o negli algoritmi;
- impatti indiretti su lavoratori, utenti o terzi;
- utilizzi non coerenti con i principi di parità di trattamento.

Il monitoraggio dei bias costituisce presidio di prevenzione del rischio di condotte illecite o discriminatorie, rilevanti anche ai fini del MOG ex D.Lgs. 231/2001.

c) Tutela della salute, sicurezza e dignità dei lavoratori

L'uso dell'IA non deve determinare:

- forme di sorveglianza indebita o invasiva;
- pressioni organizzative improprie;
- effetti negativi su salute, sicurezza e benessere lavorativo.

FVGS valuta gli impatti dell'IA sui contesti di lavoro e aggiorna, ove necessario, le valutazioni dei rischi aziendali, quale misura di prevenzione dei rischi organizzativi e reputazionali.

d) Protezione dei dati e sicurezza delle informazioni

I sistemi di IA sono progettati e utilizzati nel rispetto dei principi di:

- liceità, minimizzazione e proporzionalità dei dati;
- sicurezza tecnica e organizzativa;
- prevenzione di utilizzi impropri o non autorizzati.

Il rispetto della normativa in materia di protezione dei dati costituisce presidio fondamentale ai fini della responsabilità dell'ente.

POLICY IA FVGS

e) Inclusione, accessibilità e proporzionalità

FVGS promuove un utilizzo dell'IA che:

- non escluda o penalizzi soggetti vulnerabili;
- sia proporzionato rispetto alle finalità perseguite;
- tenga conto, ove applicabile, di requisiti di accessibilità e usabilità.

Art. 5 – Governance, ruoli e responsabilità

FVGS assicura una governance dell'IA coerente con il MOG, al fine di garantire un utilizzo dell'IA conforme alla normativa, controllato e responsabilmente presidiato.

a) Indirizzo e responsabilità di vertice

Il CdA esercita funzioni di indirizzo e controllo strategico in materia di utilizzo dell'IA, approvando la presente Policy, valutando i principali rischi connessi e assicurando l'adeguatezza dei presidi organizzativi e di controllo.

La Direzione Generale è responsabile dell'attuazione della Policy, del coordinamento delle funzioni coinvolte e dell'effettiva applicazione dei presidi previsti, assicurando che l'utilizzo dei sistemi di IA avvenga in modo conforme, controllato e coerente con gli indirizzi del CdA.

b) Presidio e coordinamento

I Sistemi Informativi e Telecomunicazioni (CED), il Responsabile della Protezione dei Dati (DPO) e le Risorse Umane (HR) operano in modo coordinato, secondo le rispettive competenze, al fine di assicurare che l'utilizzo dei sistemi di IA avvenga in condizioni di sicurezza tecnica, nel rispetto della normativa in materia di protezione dei dati personali e dei diritti dei lavoratori.

In particolare:

- il **CED** è responsabile del presidio tecnico dei sistemi di IA e assicura:
 - la progettazione, integrazione e gestione tecnica dei sistemi di IA;
 - la sicurezza informatica, l'affidabilità e la continuità operativa;
 - la gestione tecnica degli accessi, delle infrastrutture e dei flussi di dati;
 - la segnalazione di criticità tecniche o anomalie di funzionamento.
- il **DPO** svolge funzioni di consulenza e sorveglianza sui profili di protezione dei dati personali connessi all'utilizzo dei sistemi di IA e:
 - supporta la valutazione dei rischi per i diritti e le libertà degli interessati;
 - supporta, per i profili di protezione dei dati personali, l'istruttoria relativa ai sistemi di IA che consentano, anche solo potenzialmente, il controllo a distanza dell'attività dei lavoratori, fornendo pareri a HR sulla conformità del trattamento, predisponendo l'informativa ai lavoratori prevista dall'art. 4, co. 3, della legge 20 maggio 1970, n. 300;
 - fornisce pareri sulla necessità e sull'esito delle valutazioni di impatto sulla protezione dei dati (DPIA);
 - opera in condizioni di autonomia e indipendenza, senza assumere responsabilità operative sui sistemi di IA.
- **HR** presidia i profili organizzativi e giuslavoristici connessi all'utilizzo dell'IA e:
 - valuta gli impatti dei sistemi di IA sui processi di lavoro e sull'organizzazione;

POLICY IA FVGS

- assicura il rispetto della normativa in materia di lavoro e dei diritti dei lavoratori;
 - contribuisce alla definizione delle misure formative e informative sull'uso dell'IA;
 - con il supporto del DPO, cura la procedura di accordo collettivo con le rappresentanze sindacali aziendali o, in subordine, la richiesta di autorizzazione all'Ispettorato Nazionale del Lavoro, ai sensi dell'art. 4, co. 1, della legge 20 maggio 1970, n. 300, qualora il sistema di IA consenta, anche solo potenzialmente, il controllo a distanza dell'attività dei lavoratori;
 - supporta l'analisi degli impatti occupazionali e organizzativi.
- le singole **Aree aziendali** esercitano un presidio di primo livello sull'utilizzo dei sistemi di IA nei processi di rispettiva competenza. In particolare, ciascuna Area:
 - assicura che l'utilizzo dei sistemi di IA sia coerente con le finalità del processo e con le disposizioni della presente Policy;
 - garantisce l'effettiva supervisione umana degli output prodotti dai sistemi di IA;
 - risponde degli impatti organizzativi e operativi derivanti dall'utilizzo dell'IA nel processo di competenza;
 - segnala tempestivamente alle funzioni competenti eventuali criticità, anomalie o utilizzi non conformi.

Tale presidio non sostituisce né limita le competenze delle funzioni di presidio tecnico, privacy e controllo, ma si integra nel sistema complessivo di controllo interno.

c) Utilizzo operativo

L'**utente operativo** utilizza i sistemi di IA nell'ambito delle proprie mansioni, esclusivamente per finalità lavorative lecite e dichiarate. Egli valuta criticamente gli output prodotti dall'IA, riconoscendone il ruolo di supporto e non decisionale, e non assume decisioni autonome con effetti giuridici o rilevanti sulle persone. L'utente segnala tempestivamente anomalie, errori o utilizzi impropri alla Direzione e alle funzioni competenti.

HR, in coordinamento con le funzioni competenti, assicura che gli utenti operativi dei sistemi di IA ricevano adeguata informazione e formazione sull'uso responsabile dell'IA, sui limiti di utilizzo, sui rischi connessi e sulle responsabilità previste dalla presente Policy. La formazione è finalizzata a garantire la consapevolezza del ruolo di supporto dell'IA, il corretto esercizio della supervisione umana e la capacità di riconoscere e segnalare anomalie o utilizzi non conformi.

La formazione sull'uso responsabile dell'IA contribuisce, inoltre, a ridurre incertezze operative e percezioni di rischio connesse all'introduzione di nuove tecnologie, favorendo una maggiore consapevolezza e un utilizzo più sereno degli strumenti digitali, anche in relazione ai profili di benessere organizzativo e di stress lavoro correlato.

Art. 6 – Registro e mappatura dei sistemi IA

FVGS istituisce e mantiene un **Registro dei sistemi di Intelligenza Artificiale** (denominato M 14.09 Registro IA), quale strumento di governo, controllo e accountability dell'utilizzo dell'IA all'interno dell'organizzazione.

Il M 14.09 Registro IA è inteso quale inventario strutturato e aggiornato dei sistemi di IA utilizzati all'interno dell'organizzazione e consente di assicurare la tracciabilità dei sistemi impiegati, delle relative finalità, dei processi aziendali impattati e dei principali profili di rischio.

Per ciascun sistema di IA il M 14.09 Registro IA riporta la denominazione e la descrizione del sistema; il fornitore e la natura della soluzione; le finalità perseguite e i processi aziendali interessati; la categoria di rischio attribuita; gli eventuali incidenti o criticità rilevati; la data di inserimento, di ultimo aggiornamento e di eventuale dismissione del sistema.

POLICY IA FVGS

Il M 14.09 Registro IA è disciplinato nell'ambito dell'Istruzione denominata I 14.05 Utilizzo IA. Il M 14.09 Registro IA è mantenuto costantemente aggiornato ed è reso disponibile alle funzioni di presidio e controllo competenti, quale base informativa per le valutazioni di conformità, le attività di monitoraggio e i flussi informativi previsti dal sistema di controllo interno. Le informazioni contenute nel M 14.09 Registro IA concorrono, per la parte di competenza, all'adempimento degli obblighi di pubblicazione nella sezione "Società Trasparente" del sito istituzionale ai sensi dell'art. 30, co. 5, del D.Lgs. 36/2023 e del D.Lgs. 33/2013 e s.m.i..

Art. 7 – Classificazione del rischio e requisiti minimi

FVGS classifica i sistemi di IA utilizzati all'interno dell'organizzazione in base alle **categorie di rischio previste dal Regolamento (UE) 2024/1689 (AI Act)**, in coerenza con i principi e le disposizioni della Legge 23 settembre 2025, n. 132.

La classificazione del rischio costituisce presupposto essenziale per la valutazione di ammissibilità dei sistemi di IA, per la definizione dei presidi applicabili e per l'attivazione delle valutazioni di impatto previste dalla presente Policy.

In particolare, i **sistemi di IA** sono ricondotti alle seguenti categorie:

- **a rischio inaccettabile** sono quelli il cui utilizzo è vietato dal Regolamento (UE) 2024/1689 in quanto incompatibile con i diritti fondamentali e con i valori dell'ordinamento. Possono includere, ad esempio, sistemi destinati a forme di sorveglianza generalizzata o di profilazione automatizzata dei lavoratori o degli utenti, ovvero sistemi idonei a incidere sui diritti fondamentali in modo incompatibile con i principi dell'ordinamento. Tali sistemi non possono essere adottati né utilizzati da FVGS in alcuna forma o contesto.
- **ad alto rischio** sono quelli che, per le loro finalità o per il contesto di utilizzo, possono incidere in modo significativo su diritti fondamentali, lavoro, salute, sicurezza o accesso a servizi essenziali. Possono includere, a titolo esemplificativo, sistemi utilizzati a supporto di processi che incidono su diritti o posizioni giuridiche rilevanti, quali la valutazione di performance lavorative, l'assegnazione di incarichi o priorità operative, ovvero l'accesso a servizi o benefici, ove l'IA abbia un ruolo significativo nel processo decisionale. L'utilizzo di tali sistemi è subordinato al rispetto di requisiti rafforzati in termini di valutazione preventiva dei rischi, documentazione, tracciabilità, supervisione umana effettiva e monitoraggio continuo, secondo quanto previsto dalla normativa europea e dalla presente Policy. Costituiscono in ogni caso sistemi ad alto rischio quelli individuati dall'articolo 6 e dall'Allegato III del Regolamento (UE) 2024/1689, cui FVGS fa riferimento ai fini della classificazione.
- **a rischio limitato** sono sistemi che presentano rischi circoscritti e che richiedono specifici obblighi di trasparenza e informazione, al fine di consentire agli utenti di comprendere il ruolo dell'IA e di esercitare un controllo consapevole sugli output prodotti. Possono includere sistemi di supporto alle attività informative o comunicative, quali strumenti di assistenza virtuale, sistemi di supporto alla redazione di contenuti o alla classificazione preliminare di richieste, nei quali l'interazione con l'IA è chiaramente riconoscibile e gli output non producono effetti rilevanti senza un intervento umano.
- **a rischio minimo o nullo** sono quelli che non comportano rischi significativi per diritti o interessi giuridicamente rilevanti e che possono essere utilizzati nel rispetto dei principi generali di cui alla presente Policy, ferma restando la supervisione umana e la responsabilità dell'ente. Possono includere strumenti di supporto interno a basso impatto, quali applicazioni di ottimizzazione di flussi informativi, analisi statistiche aggregate o strumenti di automazione di attività meramente tecniche o ripetitive, che non incidono su diritti, persone o decisioni rilevanti.

POLICY IA FVGS

La classificazione del rischio è effettuata in fase di introduzione del sistema e riesaminata in caso di modifiche rilevanti delle funzionalità, delle modalità di utilizzo o del contesto organizzativo. Gli esiti della classificazione sono documentati e costituiscono parte integrante del M 14.09 Registro IA.

Al fine di garantire l'oggettività e la tracciabilità, da applicarsi in sede di introduzione del sistema di IA e in occasione di riesame, la classificazione del rischio è effettuata utilizzando apposita checklist (M 14.08 Richiesta e valutazione sistema IA), che considera almeno i seguenti elementi:

- impatto su diritti e interessi di persone fisiche;
- grado di autonomia del sistema e livello di intervento umano;
- tipologia dei dati trattati (personali e aziendali);
- impatti sull'organizzazione del lavoro e sui lavoratori;
- rischi tecnici, di sicurezza e affidabilità.

Gli esiti della valutazione sono formalizzati e motivati nel modulo M 14.08 Richiesta e valutazione sistema IA e costituiscono parte integrante del M 14.09 Registro IA.

Art. 8 – Valutazioni di impatto e autorizzazione all'uso

In coerenza con l'Art. 7, FVGS stabilisce che:

- I. i sistemi riconducibili a **rischio inaccettabile** non sono in alcun caso ammissibili e, pertanto, non possono formare oggetto di autorizzazione;
- II. i sistemi **ad alto rischio** sono assoggettati a un regime di valutazione e autorizzazione rafforzato;
- III. per i sistemi **a rischio limitato e minimo o nullo** si applicano presidi e verifiche proporzionati, ferma restando la supervisione umana e il rispetto dei principi inderogabili di cui all'Art. 4.

Prima dell'avvio in esercizio e in occasione di modifiche rilevanti delle funzionalità, delle modalità d'uso o del contesto organizzativo, FVGS effettua, in relazione alla categoria di rischio individuata, le **valutazioni di impatto** ritenute necessarie, includendo almeno: la valutazione dei profili privacy e dei diritti (con DPIA ove applicabile) e la valutazione degli impatti organizzativi e occupazionali. Tali valutazioni costituiscono condizione per l'adozione consapevole del sistema e per la definizione delle misure di mitigazione e controllo.

L'autorizzazione all'uso è rilasciata solo a seguito della verifica della sussistenza e adeguatezza dei presidi minimi di compliance e controllo previsti dalla presente Policy, con particolare riguardo alla corretta configurazione della supervisione umana, alla tracciabilità/logging delle attività e degli output rilevanti e alla predisposizione di misure di gestione delle anomalie e degli incidenti. La messa in esercizio è, pertanto, subordinata alla dimostrabilità documentale di tali presidi, anche ai fini dell'accountability e dei controlli interni.

Laddove il sistema sia classificato **ad alto rischio** ai sensi dell'Art. 7, FVGS assicura un livello rafforzato di documentazione, tracciabilità, supervisione umana effettiva e monitoraggio continuo, coerentemente con i requisiti previsti dalla normativa europea e con le misure di audit e mitigazione stabilite dalla presente Policy.

Le valutazioni di impatto sono documentate mediante gli strumenti operativi aziendali e integrate nel processo di autorizzazione, assicurando la tracciabilità delle decisioni, delle verifiche effettuate e delle eventuali prescrizioni adottate.

Art. 9 – Monitoraggio, verifiche e misure di mitigazione

FVGS assicura un monitoraggio proporzionato dell'utilizzo dei sistemi di IA, coerente con la categoria di rischio individuata ai sensi dell'Art. 7 e con le valutazioni di impatto effettuate ai sensi dell'Art. 8.

POLICY IA FVGS

Il monitoraggio è finalizzato a verificare, nel tempo, che l'utilizzo dei sistemi di IA resti conforme alle finalità dichiarate, ai presidi individuati e ai principi inderogabili di cui alla presente Policy, tenendo conto dell'evoluzione del contesto organizzativo, tecnologico e normativo.

Ai fini della presente Policy, per "incidente di Intelligenza Artificiale" si intende qualsiasi evento, malfunzionamento, utilizzo improprio o effetto inatteso derivante dall'utilizzo di un sistema di IA, idoneo a determinare o a poter determinare:

- violazioni normative o contrattuali;
- trattamenti illeciti o non conformi dei dati personali;
- effetti discriminatori o distorsivi nei confronti di persone o gruppi;
- decisioni errate o fuorvianti con impatti rilevanti su processi, servizi o attività aziendali;
- compromissione della sicurezza delle informazioni o dei sistemi aziendali;
- utilizzi non autorizzati o non coerenti con le finalità dichiarate;
- impatti negativi significativi sui lavoratori, sull'organizzazione o sugli utenti dei servizi.

Costituiscono, in particolare, incidenti rilevanti:

- anomalie degli output che possano comportare decisioni errate o distorsioni rilevanti;
- utilizzo del sistema in assenza di autorizzazione o al di fuori delle finalità approvate;
- inserimento o trattamento non autorizzato di dati personali o informazioni riservate;
- comportamenti discriminatori o bias evidenziati nel funzionamento del sistema;
- malfunzionamenti tecnici con impatto sulla continuità operativa o sulla sicurezza.

In relazione al livello di rischio del sistema, il monitoraggio può includere, in forma non continuativa e non automatica, attività di verifica sull'adeguatezza della supervisione umana, sulla coerenza degli output rispetto alle finalità del processo e sull'eventuale insorgenza di criticità o anomalie rilevanti.

FVGS assicura che eventuali criticità, malfunzionamenti, deviazioni significative o utilizzi non conformi dei sistemi di IA siano tempestivamente gestiti, anche mediante l'adozione di misure correttive o di mitigazione proporzionate, fino alla sospensione o dismissione del sistema, ove necessario.

Le attività di monitoraggio e le misure adottate sono documentate nel modulo M 14.08 Richiesta e valutazione sistema IA in modo essenziale e costituiscono base informativa per il riesame periodico della Policy e per i flussi informativi verso le funzioni di presidio e controllo competenti, nonché per i flussi informativi periodici verso l'Organismo di Vigilanza. In particolare, sono oggetto di comunicazione ad evento all'OdV. gli incidenti, le anomalie rilevanti, le violazioni dei divieti di cui all'art. 10.

Art. 10 – Divieti

FVGS stabilisce i seguenti divieti inderogabili nell'utilizzo dei sistemi di IA:

- È fatto divieto assoluto di adottare o utilizzare sistemi di IA riconducibili alle categorie di rischio inaccettabile ai sensi dell'Art. 7, in quanto incompatibili con i diritti fondamentali e con i principi dell'ordinamento.
- È vietato utilizzare sistemi di IA per finalità di sorveglianza dei lavoratori oltre i limiti consentiti dalla legge o per modalità di controllo non dichiarate, indirette o invasive, in violazione della normativa lavoristica e dei principi di proporzionalità e trasparenza. Qualora il sistema di IA consenta, anche solo potenzialmente, il controllo a distanza dell'attività dei lavoratori, la sua introduzione è subordinata al preventivo accordo collettivo con le rappresentanze sindacali aziendali o, in subordine, all'autorizzazione dell'Ispettorato Nazionale del Lavoro, ai sensi dell'art. 4, co. 1, della legge 300/1970 e s.m.i.. In ogni caso, i lavoratori interessati sono preventivamente informati delle caratteristiche e delle modalità di funzionamento del sistema, delle finalità perseguite e delle tipologie di dati eventualmente trattati, nel rispetto dell'art. 4, co.

POLICY IA FVGS

3, della medesima legge. La procedura viene gestita da HR, con il supporto del DPO, come indicato sopra nell'art. 5.

- È vietato adottare o utilizzare sistemi di IA idonei a indagare, anche indirettamente, sulle opinioni politiche, religiose o sindacali dei lavoratori, ovvero su fatti non rilevanti ai fini della valutazione dell'attitudine professionale, ai sensi dell'art. 8 della legge 20 maggio 1970, n. 300. È in particolare vietato l'impiego di software di analisi del linguaggio nei colloqui di selezione idonei a valutare tratti di personalità o predisposizioni personali, in quanto suscettibili di rivelare opinioni o caratteristiche non pertinenti.
- È vietato adottare o utilizzare sistemi di IA che producano effetti discriminatori o disparità di trattamento tra i lavoratori per ragioni di sesso, età, orientamento, condizioni personali o sociali, ovvero convinzioni personali, sindacali, politiche o religiose. I sistemi sono preventivamente e periodicamente testati al fine di individuare e correggere correlazioni idonee a produrre tali effetti, in coerenza con l'art. 15 della legge 20 maggio 1970, n. 300, che sancisce la nullità degli atti discriminatori.
- È vietato utilizzare sistemi di IA per l'adozione di decisioni esclusivamente automatizzate che producano effetti giuridici o incidano in modo rilevante sulle persone, in particolare in materia di assunzione, valutazione, assegnazione di incarichi, premi, sanzioni disciplinari o cessazione del rapporto di lavoro. In tali ambiti, la responsabilità decisionale resta in ogni caso in capo a un soggetto umano.
- È fatto divieto di utilizzare sistemi di IA per finalità diverse da quelle dichiarate e autorizzate ai sensi della presente Policy, nonché di impiegare tali sistemi in assenza dei presidi di supervisione umana, tracciabilità e controllo previsti.
- È infine vietato l'addestramento o il riaddestramento di modelli di IA mediante l'utilizzo di dati personali dei lavoratori o di altri soggetti in assenza di un'adeguata base giuridica e delle necessarie valutazioni di impatto, ove applicabili.

Le violazioni dei divieti di cui al presente articolo sono valutate ai fini dell'attivazione dei presidi previsti dal sistema di controllo interno, incluse le misure disciplinari e le eventuali responsabilità rilevanti ai sensi del D.Lgs. 231/2001.

Art. 11 – Gestione fornitori e contratti

FVGS assicura che la selezione e la gestione dei fornitori di soluzioni di IA avvengano nel rispetto dei principi di legalità, trasparenza, correttezza, proporzionalità e responsabilità, nonché delle disposizioni del D.Lgs. 36/2023, in coerenza con la presente Policy e con il sistema di controllo interno. L'approvvigionamento di sistemi di IA è effettuato nel rispetto delle procedure applicabili in ragione della tipologia e del valore dell'affidamento, con particolare attenzione alla definizione dei requisiti tecnici e funzionali nei capitolati, alla previsione di clausole contrattuali che garantiscano la portabilità dei dati al termine del rapporto, i diritti di audit e verifica da parte di FVGS, la cooperazione del fornitore nelle attività di monitoraggio e gestione degli incidenti, nonché la disciplina della titolarità dei dati e degli output realizzati nel corso dell'esecuzione contrattuale.

In attuazione di quanto disposto dall'art. 30 del Codice dei Contratti Pubblici, l'utilizzo di procedure automatizzate – inclusi strumenti digitali e sistemi di IA – nelle fasi di selezione, aggiudicazione, stipula, esecuzione e monitoraggio dei contratti pubblici è consentito solo nel rispetto dei principi di legalità, imparzialità, trasparenza, proporzionalità ed efficienza. In particolare, tali procedure devono:

- conformarsi alla normativa europea e nazionale vigente, garantendo piena tracciabilità, verificabilità e ricostruibilità di tutte le operazioni;
- assicurare il rispetto del principio di parità di trattamento e di non discriminazione attraverso criteri di valutazione chiari, documentati e comprensibili, nonché mediante un controllo umano significativo, effettivo e documentato in ogni fase decisionale automatizzata;

POLICY IA FVGS

- assicurare, ai sensi dell'art. 30, co. 2, lett. a), del D.Lgs. 36/2023, la disponibilità del codice sorgente, della documentazione tecnica e di ogni altro elemento utile a comprendere la logica di funzionamento delle soluzioni tecnologiche adottate, anche ai fini dell'esercizio dei diritti di accesso e della verifica di conformità;
- assicurare, ai sensi dell'art. 30, co. 2, lett. b), del D.Lgs. 36/2023, che i capitolati di gara includano i requisiti di manutenzione e aggiornamento del sistema di IA per l'intera durata del contratto, con indicazione delle modalità di erogazione degli aggiornamenti, dei tempi di intervento, dei livelli minimi di servizio garantiti e delle relative conseguenze in caso di inadempimento;
- garantire che nessuna decisione che produca effetti giuridici rilevanti nei confronti di candidati od operatori economici possa essere adottata in modo integralmente automatizzato, salvo nei casi espressamente consentiti dalla legge e previa verifica dell'assenza di rischi discriminatori, di bias algoritmico o di distorsioni della concorrenza;
- adottare misure tecniche e organizzative idonee a prevenire, rilevare e mitigare eventuali anomalie, errori, criticità o vulnerabilità connesse all'impiego di soluzioni automatizzate, inclusi meccanismi periodici di audit e riesame.

L'affidamento di soluzioni di IA a fornitori esterni è subordinato a una valutazione preventiva dell'adeguatezza del fornitore sotto il profilo dell'affidabilità tecnica, della conformità normativa e della capacità di garantire presidi adeguati in materia di sicurezza, tutela dei dati, supervisione umana e gestione dei rischi.

I rapporti contrattuali relativi a sistemi di IA prevedono, in misura proporzionata alla tipologia e al livello di rischio del sistema, **clausole etiche e di integrità** idonee a richiamare:

- il rispetto dei diritti fondamentali, dei principi di non discriminazione e di tutela della dignità della persona;
- il divieto di utilizzi impropri, illeciti o non conformi alle finalità dichiarate;
- l'impegno del fornitore a operare in coerenza con i principi della presente Policy e con il MOG ex D.Lgs. 231/2001 adottato da FVGS.

I contratti prevedono inoltre clausole idonee a disciplinare, in modo proporzionato:

- la trasparenza e la documentabilità delle funzionalità del sistema di IA;
- la cooperazione del fornitore nelle attività di controllo, verifica e gestione delle anomalie;
- le responsabilità e gli obblighi in caso di malfunzionamenti, incidenti o utilizzi non conformi.

I contratti relativi a sistemi di IA prevedono, altresì, clausole idonee a prevenire condizioni di dipendenza tecnologica dal fornitore, mediante la previsione di requisiti di interoperabilità e compatibilità con standard aperti, l'obbligo del fornitore di fornire documentazione tecnica sufficiente a garantire la transizione verso soluzioni alternative senza perdita di dati o funzionalità critiche, nonché la disponibilità dei dati in formato aperto o standard al termine del rapporto.

Con riferimento ai profili di **sicurezza delle informazioni e cybersicurezza**, FVGS assicura che i fornitori di soluzioni di IA dimostrino l'adozione di misure tecniche e organizzative adeguate, anche mediante il possesso di certificazioni, attestazioni o standard di sicurezza riconosciuti, ove applicabili, o mediante il rispetto di requisiti equivalenti coerenti con il quadro normativo vigente, incluso quello derivante dalla Direttiva (UE) 2022/2555 (NIS 2), ove pertinente al fornitore e al servizio erogato.

Laddove i sistemi di IA comportino trattamenti di dati personali, FVGS assicura che i rapporti con i fornitori siano regolati nel rispetto della normativa in materia di protezione dei dati, inclusa la corretta qualificazione dei ruoli e delle responsabilità delle parti e l'adozione delle misure di sicurezza previste.

POLICY IA FVGS

La gestione dei fornitori di soluzioni di IA costituisce presidio rilevante ai fini della prevenzione dei rischi legali, organizzativi, reputazionali e di responsabilità dell'ente, ed è parte integrante del sistema di controllo interno di FVGS.

Art. 12 – Conservazione documentale

FVGS assicura la corretta **conservazione e tracciabilità della documentazione** relativa ai sistemi di IA adottati o utilizzati, quale presidio di accountability, di controllo interno e di dimostrabilità della conformità alla normativa applicabile.

Sono oggetto di conservazione, in forma proporzionata e pertinente, la documentazione relativa al M 14.09 Registro IA, alle classificazioni di rischio, alle valutazioni di impatto, alle attività di monitoraggio, alle decisioni rilevanti assunte con il supporto dell'IA, nonché agli eventuali incidenti, criticità o misure di mitigazione adottate.

La documentazione è conservata nel rispetto:

- delle disposizioni normative vigenti;
- degli atti e regolamenti aziendali in materia di gestione documentale, trasparenza e controllo interno;
- delle convenzioni, accordi o vincoli contrattuali applicabili, ove pertinenti.

La documentazione conservata è resa disponibile, nei limiti delle rispettive competenze, alle funzioni di presidio e controllo, all'OdV, al RPCT e agli organi competenti, anche ai fini delle attività di verifica, audit e riesame della presente Policy.

La documentazione relativa ai sistemi IA (M 14.09 Registro IA, valutazioni, audit, log, verbali e decisioni) è conservata per almeno 5 anni o per il diverso termine previsto dalla normativa applicabile.

Art. 13 – Gestione dei dati personali nell'utilizzo dei sistemi di Intelligenza Artificiale

FVGS assicura che l'utilizzo dei sistemi di IA che comportano il trattamento di dati personali avvenga nel pieno rispetto del **Regolamento (UE) 2016/679 (GDPR)**, della normativa nazionale applicabile dei principi di cui alla presente Policy e dei Regolamenti aziendali in materia.

I trattamenti di dati personali connessi all'impiego dei sistemi di IA sono effettuati nel rispetto dei principi di liceità, correttezza, trasparenza, minimizzazione, proporzionalità e sicurezza, nonché del principio di accountability del titolare del trattamento.

Prima dell'introduzione o della modifica significativa di sistemi di IA che comportino trattamenti di dati personali, FVGS valuta la necessità di effettuare una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** ai sensi dell'art. 35 del GDPR, tenendo conto della natura, delle finalità e dei rischi del trattamento. Il DPO fornisce consulenza e supporto in relazione a tali valutazioni, nel rispetto della propria autonomia e indipendenza.

È fatto divieto di utilizzare sistemi di IA per trattamenti di dati personali in assenza di un'idonea base giuridica o in violazione delle finalità dichiarate, nonché di impiegare dati personali per l'addestramento o il riaddestramento dei modelli di IA al di fuori dei casi consentiti dalla normativa applicabile.

FVGS assicura che i diritti degli interessati siano garantiti anche in relazione ai trattamenti effettuati mediante sistemi di IA, inclusi i diritti di informazione, accesso, rettifica, cancellazione, limitazione e opposizione, nonché le garanzie previste in materia di decisioni automatizzate.

La gestione dei dati personali nell'ambito dei sistemi di IA si coordina con le disposizioni della presente Policy, con il Registro dei trattamenti, con il M 14.09 Registro IA e con gli atti e regolamenti aziendali in materia di protezione dei dati e sicurezza delle informazioni.

Art. 14 – Formazione

POLICY IA FVGS

FVGS assicura formazione iniziale e periodica in materia di utilizzo responsabile dell'IA, quale presidio essenziale di prevenzione dei rischi legali, organizzativi e reputazionali connessi all'adozione di tali tecnologie.

La formazione è modulata in modo proporzionato ai ruoli e alle responsabilità e riguarda, in particolare, i soggetti coinvolti nell'adozione, nella gestione e nell'utilizzo dei sistemi di IA, inclusi i responsabili di processo, gli utenti operativi e le funzioni di presidio.

I contenuti formativi sono orientati a garantire la conoscenza:

- dei **principi inderogabili** di cui alla presente Policy;
- dei **limiti di utilizzo** dei sistemi di IA e del divieto di decisioni esclusivamente automatizzate con effetti rilevanti sulle persone;
- dei principali **rischi connessi all'uso dell'IA**, inclusi i profili di tutela dei dati personali, dei diritti dei lavoratori e di non discriminazione;
- delle modalità di **segnalazione di anomalie o utilizzi non conformi**.

HR, in coordinamento con le funzioni competenti e con il DPO per i profili privacy, assicura la pianificazione, l'erogazione e la tracciabilità degli interventi formativi, in coerenza con gli atti e le procedure aziendali in materia di formazione, come descritto nell'art. 5.

Art. 15 – Riesame e aggiornamento

La presente Policy è oggetto di riesame periodico, al fine di assicurarne la costante adeguatezza rispetto all'evoluzione del contesto normativo, tecnologico e organizzativo, nonché alla concreta esperienza applicativa dei sistemi di IA all'interno di FVGS.

Il riesame è effettuato, di norma, con cadenza almeno annuale ed è comunque attivato in presenza di:

- significative evoluzioni normative o regolamentari in materia di IA, protezione dei dati personali, lavoro o responsabilità dell'ente;
- introduzione di nuovi sistemi di IA o modifiche rilevanti di quelli esistenti;
- criticità, incidenti o utilizzi non conformi emersi in fase di monitoraggio;
- modifiche organizzative o di processo che incidano sull'utilizzo dell'IA.

Il riesame tiene conto delle risultanze delle attività di monitoraggio, delle valutazioni di impatto effettuate, delle segnalazioni ricevute e dei flussi informativi verso le funzioni di presidio e controllo, al fine di valutare l'adeguatezza dei principi, dei presidi e delle responsabilità previsti dalla presente Policy.

Gli eventuali aggiornamenti della Policy sono approvati dal CdA e comunicati alle strutture interessate secondo le modalità previste dagli atti e regolamenti aziendali applicabili.

La Società assicura che l'adozione e l'utilizzo di sistemi di Intelligenza Artificiale avvengano nel rispetto del quadro normativo vigente, ivi incluso il Modello di Organizzazione, Gestione e Controllo adottato ai sensi del D.Lgs. 231/2001 e s.m.i. e della normativa in materia di protezione dei dati personali, compresa quella di cui all'utilizzo dei sistemi di IA è subordinato alla preventiva valutazione dei profili di rischio e di conformità, con il coinvolgimento delle funzioni competenti, incluso il Responsabile della protezione dei dati (DPO).

Resta fermo che l'adozione della presente Policy non pregiudica la necessità di successivi adeguamenti del Modello 231, delle procedure interne e della documentazione privacy, che saranno effettuati ove necessario in relazione ai rischi e agli impatti derivanti dall'utilizzo dei sistemi di IA.

POLICY IA FVGS

In considerazione della natura di società in house, la Società garantisce la coerenza della presente Policy con gli indirizzi eventualmente adottati dalla Regione nell'esercizio del controllo analogo e provvede, ove necessario, al relativo adeguamento.

Art. 16 – Entrata in vigore e diffusione

La presente Policy è stata approvata dal CdA durante la seduta del nn/nn/20nn ed entra in vigore il giorno successivo alla sua approvazione ed è vincolante per tutti i soggetti rientranti nel relativo ambito di applicazione. Nelle more dell'approvazione formale delle modifiche da parte del CdA, la Direzione Generale è autorizzata ad adottare, le misure attuative provvisorie che si rendano necessarie per assicurare la conformità della Policy a sopravvenute disposizioni normative imperative. Tali misure provvisorie sono sottoposte a ratifica del CdA alla prima seduta utile.

FVGS assicura la diffusione e la conoscibilità della Policy nei confronti del personale e dei soggetti esterni interessati, mediante i canali aziendali e gli strumenti previsti dagli atti e dai regolamenti interni, anche al fine di garantirne l'effettiva applicazione.

La Policy è resa disponibile secondo modalità coerenti con il sistema di gestione aziendale ed è comunicata alle parti interessate, nonché pubblicata sull'Intranet aziendale, ferma restando l'integrazione con le attività di informazione e formazione previste dalla presente Policy e dagli atti aziendali applicabili.

L'osservanza della presente Policy costituisce parte integrante degli obblighi connessi allo svolgimento delle attività lavorative e professionali in FVGS, nel rispetto delle responsabilità e delle competenze attribuite ai diversi ruoli organizzativi.

Le violazioni della stessa possono comportare misure disciplinari e ulteriori responsabilità previste dalla normativa e dal MOG ex D.Lgs. 231/2001.