REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	CDA DEL 16.05.2026	ADOZIONE

SOMMARIO

1 PREMESSA E SCOPO DELLA POLICY IA

La presente Policy stabilisce le linee guida per promuovere la diffusione di un'Intelligenza Artificiale (IA) antropocentrica e affidabile all'interno di IDRAGEST S.r.l.

L'obiettivo, infatti, è garantire un livello elevato di protezione della salute, della sicurezza e dei diritti fondamentali delle persone, promuovendo al contempo l'innovazione responsabile, in linea con quanto stabilito dall'Articolo 1 del Regolamento (UE) 2024/1689 (AI Act).

IDRAGEST S.r.l. riconosce il valore strategico delle tecnologie di intelligenza artificiale ed il loro potenziale per il miglioramento dei propri processi operativi, della qualità dei servizi offerti e della competitività aziendale, a condizione che il suo utilizzo avvenga nel pieno rispetto dei valori etici, dei diritti fondamentali delle persone e del quadro normativo vigente.

Con la presente Policy, IDRAGEST formalizza il proprio impegno nell'adozione di principi etici conformi agli standard internazionali e al diritto dell'Unione Europea, tra i quali i principi OCSE sull'IA, le Linee Guida del G7 sull'IA responsabile, le Linee Guida per un'IA affidabile dell'High-Level Expert Group on AI della Commissione Europea, il Regolamento (UE) 2024/1689 (AI Act) e il Regolamento (UE) 2016/679 (GDPR).

La Policy si inserisce nel più ampio sistema di governance aziendale adottato da IDRAGEST, e si coordina con il Codice Etico, il Modello di Organizzazione Gestione e Controllo ex D.Lgs. 8 giugno 2001, n. 231 e la disciplina contrattuale in materia di IA contenuta nelle Condizioni Generali di Contratto.

Il documento è reso disponibile tramite la intranet aziendale e comunicato a tutti i dipendenti, collaboratori e soggetti che operano per conto di IDRAGEST.

2 DEFINIZIONI

AI FINI DELLA PRESENTE POLICY E AI SENSI DELL'ARTICOLO 3 DEL REGOLAMENTO (UE) 2024/1689 (AI ACT), SI ADOTTANO LE SEGUENTI DEFINIZIONI:

SISTEMA DI IA: sistema automatizzato progettato per funzionare con livelli di autonomia variabili, che può presentare capacità di adattamento e che — per obiettivi espliciti o impliciti — genera output quali previsioni, raccomandazioni, decisioni o contenuti in grado di influenzare ambienti fisici o virtuali.

«CHATGPT BUSINESS/ENTERPRISE/EDU»: versioni di ChatGPT sviluppate da OpenAI ed autorizzate all'uso aziendale, caratterizzate da garanzie contrattuali di non utilizzo dei dati degli utenti per l'addestramento

dei modelli, da funzionalità avanzate di amministrazione e controllo degli accessi e da livelli di sicurezza rafforzati rispetto alla versione consumer gratuita.

«IA GENERATIVA»: sistema di intelligenza artificiale in grado di generare contenuti testuali, grafici, audio o multimediali a partire da istruzioni fornite dall'utente (prompt), ai sensi dell'art. 3, par. 1, n. 63, del Regolamento (UE) 2024/1689 (AI Act).

DEPLOYER: la persona fisica o giuridica che utilizza un sistema di IA sotto la propria responsabilità ed autorità, a scopo non personale. Nell'ambito della presente Policy, il Deployer è IDRAGEST S.r.l. e, per estensione funzionale, i suoi dipendenti e collaboratori autorizzati.

ALFABETIZZAZIONE IN MATERIA DI IA: le competenze, le conoscenze e le capacità che consentono una diffusione informata dei sistemi di IA, nonché la consapevolezza critica dei loro benefici, rischi e limiti.

«PROMPT»: istruzione, domanda o testo fornito dall'utente al sistema di IA generativa per ottenere un output.

«DATI RISERVATI»: qualsiasi informazione confidenziale di IDRAGEST o dei suoi Clienti, partner o fornitori; i dati personali; i segreti industriali; i dati tecnici; know-how; i progetti ingegneristici; le offerte commerciali ed economiche e qualsiasi altra informazione non destinata alla divulgazione pubblica.

«UTENTE AUTORIZZATO»: soggetto abilitato all'utilizzo di ChatGPT Business/Enterprise/Edu nell'ambito delle attività aziendali, previa accettazione della presente Policy.

«OUTPUT»: qualsiasi contenuto, informazione, elaborazione o risultato generato dal sistema di IA in risposta a un prompt dell'utente.

«RESPONSABILE IA»: il soggetto designato da IDRAGEST quale referente interno per la governance dei sistemi di intelligenza artificiale, responsabile dell'attuazione e del monitoraggio della presente Policy.

DESTINATARI DELLA POLICY IA: tutti i soggetti tenuti al rispetto della presente Policy, ivi inclusi dipendenti, collaboratori, consulenti, e qualsiasi altro soggetto che operi, a qualsiasi titolo, per conto di IDRAGEST nell'ambito delle attività disciplinate dalla presente Policy.

3 AMBITO DI APPLICAZIONE E DESTINATARI

La presente Policy si applica a tutti i dipendenti, collaboratori, consulenti e qualsiasi altro soggetto che operi, a qualsiasi titolo, per conto di IDRAGEST S.r.l. e che, nell'esercizio delle proprie funzioni, interagiscano con sistemi di Intelligenza Artificiale, anche per finalità accessorie o occasionali.

I soli strumenti di IA generativa autorizzati all'interno dell'azienda sono ChatGPT nelle versioni Business, Enterprise ed Edu. L'utilizzo di qualsiasi altro strumento di IA — inclusi modelli locali installati su dispositivi personali, versioni consumer gratuite e applicazioni non esplicitamente approvate — è vietato e deve essere preventivamente sottoposto all'approvazione del Responsabile IA.

3 BIS QUADRO NORMATIVO DI RIFERIMENTO

3.1 NORMATIVA DELL'UNIONE EUROPEA

La presente Policy è adottata in conformità al seguente quadro normativo dell'Unione Europea, che costituisce il fondamento giuridico dei principi e delle regole in essa contenuti.

3.1.1. REGOLAMENTO (UE) 2024/1689 — AI ACT. Il Regolamento introduce un quadro giuridico orizzontale fondato su un approccio basato sul rischio che classifica i sistemi di IA in quattro categorie: rischio inaccettabile (art. 5), alto rischio (artt. 6-51), rischio limitato (art. 50) e rischio minimo. I sistemi di IA per uso generale (GPAI), ivi inclusi i modelli linguistici di grandi dimensioni quali ChatGPT, sono disciplinati agli artt. 51-56. IDRAGEST, in qualità di deployer ai sensi dell'art. 3, par. 1, n. 4, è tenuta a rispettare gli obblighi dell'art. 26, tra cui: **(i)** utilizzo conforme alle istruzioni d'uso del provider; **(ii)** supervisione umana adeguata; **(iii)** misure tecniche e organizzative proporzionate al rischio; **(iv)** sospensione in caso di rischi per la salute, la sicurezza o i diritti fondamentali. L'obbligo di alfabetizzazione in materia di IA è sancito dall'art. 4. Invero, in conformità all'art. 4 del Regolamento (UE) 2024/1689 (AI Act), IDRAGEST garantisce che tutti gli Utenti Autorizzati dispongano di adeguati livelli di alfabetizzazione in materia di IA, attraverso un programma di formazione obbligatoria iniziale e aggiornamenti periodici.

3.1.2. REGOLAMENTO (UE) 2016/679 — GDPR. Il Regolamento stabilisce i principi fondamentali del trattamento dei dati personali (art. 5), i requisiti di liceità (art. 6), la disciplina delle categorie particolari di dati (art. 9), gli obblighi del titolare e del responsabile del trattamento (artt. 24-28), i diritti degli interessati (artt. 15-22), gli obblighi di notifica in caso di violazione dei dati (artt. 33-34) e la disciplina della DPIA (art. 35).

3.1.3. LINEE GUIDA PER UN'IA AFFIDABILE — HIGH-LEVEL EXPERT GROUP ON AI. La presente Policy si ispira ai principi di affidabilità, supervisione umana, sicurezza, trasparenza, equità e accountability elaborati dall'High-Level Expert Group on AI della Commissione Europea.

3.2 NORMATIVA NAZIONALE

3.2.1. D.LGS. 30 GIUGNO 2003, N. 196 — CODICE PRIVACY. Il Decreto Legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), come modificato dal Decreto Legislativo 10 agosto 2018, n. 101 di adeguamento al GDPR, disciplina il trattamento dei dati personali nel contesto nazionale. Il Codice Privacy integra e specifica le disposizioni del GDPR con riferimento a particolari categorie di trattamento e a specifici settori, tra cui il trattamento dei dati dei lavoratori (artt. 113-116) e il trattamento per finalità di ricerca scientifica e statistica.

3.2.2. D.LGS. 8 GIUGNO 2001, N. 231 — RESPONSABILITÀ AMMINISTRATIVA DEGLI ENTI. Il Decreto Legislativo 8 giugno 2001, n. 231costituisce il fondamento del sistema di compliance aziendale di IDRAGEST. Il Decreto prevede la responsabilità amministrativa degli enti per i reati commessi nel loro interesse o a loro vantaggio da soggetti apicali o sottoposti, e introduce il Modello di Organizzazione, Gestione e Controllo (MOG) quale strumento esimente. IDRAGEST si è dotata di un proprio Codice Etico e di un MOG ai sensi del D.Lgs. n. 231/2001. La presente Policy si coordina con il MOG e con il Codice Etico di IDRAGEST, garantendo che l'utilizzo di sistemi di IA non integri reati presupposto ai sensi del D.Lgs. n. 231/2001, ivi inclusi i reati di frode informatica (art. 24), i reati informatici (art. 24-bis), i reati societari (art. 25-ter) e i reati di corruzione (artt. 25 e 25-ter).

3.2.3. D.LGS. 10 FEBBRAIO 2005, N. 30 — CODICE DELLA PROPRIETÀ INDUSTRIALE. . Il Codice disciplina la tutela dei diritti di proprietà industriale, ivi inclusi i segreti commerciali. La presente Policy si coordina con l'art. 10 CGC, che riserva a IDRAGEST la piena titolarità dei diritti di proprietà industriale e intellettuale, e con l'art. 14.3 CGC, che attribuisce a IDRAGEST tutti i diritti di proprietà intellettuale sugli output generati dai modelli di IA generativa utilizzati.

3.2.4. LEGGE 22 APRILE 1941, N. 633 — LEGGE SUL DIRITTO D'AUTORE. . La Legge, come modificata dal D.Lgs. 8 novembre 2021, n. 177, pone rilevanti questioni interpretative in ordine alla titolarità dei diritti sugli output generati da sistemi di IA in assenza di un apporto creativo umano significativo.

3.3. STANDARD E LINEE GUIDA INTERNAZIONALI

3.3.1. PRINCIPI OCSE SULL'INTELLIGENZA ARTIFICIALE. I Principi OCSE del 2019, aggiornati nel 2023, identificano cinque principi fondamentali per un'IA responsabile: crescita inclusiva e benessere; valori centrati sull'essere umano ed equità; trasparenza e spiegabilità; robustezza, sicurezza e protezione; responsabilità.

3.3.2. LINEE GUIDA DEL G7 SULL'IA RESPONSABILE. Le Linee Guida adottate nell'ambito del Processo di Hiroshima del 2023 definiscono undici principi guida per lo sviluppo e l'utilizzo responsabile dell'IA

avanzata, tra cui mitigazione dei rischi, trasparenza, protezione dei dati personali, sicurezza informatica, supervisione umana e responsabilità.

3.4 COORDINAMENTO CON LE CONDIZIONI GENERALI DI CONTRATTO DI IDRAGEST

La presente Policy costituisce parte integrante del sistema contrattuale di IDRAGEST e si coordina con le seguenti disposizioni delle Condizioni Generali di Contratto:

(I) ART. 10 (DIRITTI DI PROPRIETÀ INDUSTRIALE E INTELLETTUALE): La presente Policy tutela il know-how, i segreti commerciali e i diritti di proprietà industriale e intellettuale di IDRAGEST, anche con riferimento agli output generati mediante sistemi di IA Generativa e al divieto di utilizzo non autorizzato del know-how di IDRAGEST per l'addestramento di modelli di IA;

(II) ART. 12 (RISERVATEZZA): la presente Policy integra gli obblighi di riservatezza contrattualmente previsti, specificando le categorie di Informazioni Confidenziali che non possono essere inserite nei prompt dei sistemi di IA e le misure di sicurezza da adottare per prevenire violazioni della riservatezza attraverso l'utilizzo di strumenti di IA generativa;

(III) ART. 13 (ETICA E ANTI-CORRUZIONE): la presente Policy si coordina con il Codice Etico e con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001 di IDRAGEST, garantendo che l'utilizzo di sistemi di IA avvenga nel pieno rispetto dei principi di onestà, imparzialità, trasparenza, lealtà e buona fede;

(IV) ART. 14 (INTELLIGENZA ARTIFICIALE): la presente Policy costituisce l'attuazione operativa della disciplina contrattuale in materia di intelligenza artificiale, specificando le modalità di utilizzo autorizzato dei sistemi di IA generativa, gli obblighi degli utenti, le misure di sicurezza e riservatezza richieste e le conseguenze delle violazioni;

(V) ART. 15 (TRATTAMENTO DEI DATI PERSONALI): la presente Policy integra la disciplina contrattuale in materia di protezione dei dati personali, con specifico riferimento al trattamento dei dati nell'ambito dell'utilizzo di sistemi di IA generativa e agli obblighi di conformità al GDPR e al D.Lgs. n. 196/2003;

(VI) ART. 9 (CLAUSOLA RISOLUTIVA ESPRESSA): la violazione degli obblighi previsti dalla presente Policy, in particolare quelli relativi al divieto di inserimento di Informazioni Confidenziali nei sistemi di IA e al rispetto del Codice Etico, può comportare la risoluzione di diritto del contratto ai sensi dell'art. 1456 c.c., in conformità a quanto previsto dall'art. 9.2, lett. ii) e vi), delle Condizioni Generali di Contratto.

3.6 AGGIORNAMENTO DEL QUADRO NORMATIVO

IDRAGEST si impegna a monitorare costantemente l'evoluzione del quadro normativo in materia di intelligenza artificiale, protezione dei dati personali e proprietà intellettuale, sia a livello nazionale che europeo e internazionale, e ad aggiornare la presente Policy in conformità alle nuove disposizioni normative man mano che queste diverranno applicabili. In particolare, IDRAGEST monitorerà l'entrata in vigore progressiva delle disposizioni dell'AI Act, che prevede un calendario di applicazione scaglionato: **(i)** divieti per i sistemi di IA a rischio inaccettabile (art. 5); **(ii)** obblighi per i sistemi di IA per uso generale (artt. 51-56); **(iii)** obblighi per i sistemi di IA ad alto rischio (artt. 6-51): applicabili dal 2 agosto 2026; **(iv)** obblighi per specifici sistemi di IA ad alto rischio (allegato I): applicabili dal 2 agosto 2027. Ogni aggiornamento della presente Policy sarà comunicato a tutti gli Utenti Autorizzati con congruo preavviso scritto, in conformità a quanto previsto dall'art. 15.2 della presente Policy, e sarà reso disponibile sulla intranet aziendale di IDRAGEST.

4 PRINCIPI GENERALI

4.1. ETICA, TRASPARENZA E FIDUCIA

IDRAGEST si impegna a garantire che tutte le applicazioni di IA siano sviluppate, implementate e utilizzate in modo etico, trasparente e responsabile, nel pieno rispetto dei diritti fondamentali della persona e in conformità ai valori sanciti dal Codice Etico aziendale e dal MOG ex D.Lgs. n. 231/2001.
In conformità all'art. 50 dell'AI Act, IDRAGEST si impegna a comunicare chiaramente ai propri clienti, collaboratori e stakeholder quando stanno interagendo con un sistema automatizzato basato sull'intelligenza artificiale, senza che tale interazione possa essere equivocata per una comunicazione umana diretta. IDRAGEST garantisce altresì che i propri sistemi di IA siano sottoposti a supervisione umana adeguata ai sensi dell'art. 26 dell'AI Act e siano gestiti secondo adeguati standard di sicurezza, affidabilità e controllo, anche in conformità alle best practice internazionali applicabili. Per la disciplina operativa della supervisione umana si rinvia all'art. 4.5.

4.2. RISPETTO DEI DIRITTI UMANI E RESPONSABILITÀ SOCIALE

IDRAGEST riconosce che l'intelligenza artificiale, se non governata con adeguata responsabilità, può costituire una minaccia per i diritti fondamentali della persona. È pertanto principio irrinunciabile della presente Policy che ogni sistema di IA adottato dalla Società sia utilizzato in modo da rispettare pienamente i diritti umani fondamentali riconosciuti dalla Carta dei Diritti Fondamentali dell'Unione

Europea, dalla Convenzione Europea per la Salvaguardia dei Diritti dell'Uomo e delle Libertà Fondamentali (CEDU) e dalla Dichiarazione Universale dei Diritti dell'Uomo delle Nazioni Unite, nonché dai principi elaborati dall'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE) in materia di intelligenza artificiale responsabile.

IN TALE PROSPETTIVA, IDRAGEST SI IMPEGNA A GARANTIRE CHE I SISTEMI DI IA ADOTTATI PROMUOVANO ATTIVAMENTE:

(I) L'INTEGRAZIONE SOCIALE, LAVORATIVA E PROFESSIONALE: i sistemi di IA devono essere progettati e utilizzati in modo da favorire l'inclusione e l'accessibilità, senza creare o amplificare forme di esclusione o marginalizzazione. In ambito lavorativo, l'intelligenza artificiale deve rappresentare uno strumento di supporto e valorizzazione delle competenze umane, migliorando l'efficienza e l'efficacia dei processi operativi — in particolare nell'analisi di grandi volumi di dati tecnici relativi alle reti idriche e fognarie oggetto dei servizi di IDRAGEST — senza sostituire il giudizio professionale umano nelle decisioni di maggiore impatto;

(II) LA RIDUZIONE DELL'ASIMMETRIA INFORMATIVA: IDRAGEST si impegna a utilizzare i sistemi di IA come strumento per ridurre, e non per amplificare, le asimmetrie informative tra la Società e i propri clienti, collaboratori e stakeholder. In conformità ai principi di trasparenza e buona fede, IDRAGEST garantisce che le informazioni generate dai sistemi di IA siano accessibili, comprensibili e verificabili da parte dei soggetti interessati;

(III) IL BENESSERE SOCIALE E AMBIENTALE: in linea con la missione aziendale di IDRAGEST nel settore dell'ottimizzazione delle reti idriche e fognarie, i sistemi di IA adottati devono contribuire al perseguimento di obiettivi di sostenibilità ambientale e di benessere collettivo, in conformità ai principi dell'Agenda 2030 delle Nazioni Unite per lo Sviluppo Sostenibile e alle Linee Guida del G7 sull'IA responsabile.

4.3. NON DISCRIMINAZIONE

IDRAGEST si impegna a prevenire l'utilizzo di sistemi di IA che possano determinare discriminazioni, trattamenti iniqui o effetti distorsivi nei confronti di persone o categorie di soggetti, nel rispetto della normativa europea e nazionale applicabile in materia di uguaglianza e non discriminazione.

4.4. PROTEZIONE DELLA PRIVACY E DEI DATI PERSONALI

Il rispetto della privacy e della protezione dei dati personali costituisce un principio fondamentale dell'utilizzo responsabile dell'intelligenza artificiale da parte di IDRAGEST, in conformità al Regolamento (UE) 2016/679 (GDPR), al D.Lgs. 30 giugno 2003, n. 196, come modificato dal D.Lgs. 10 agosto 2018, n. 101, e alle Linee Guida del Garante per la Protezione dei Dati Personali in materia di intelligenza artificiale.

IDRAGEST si impegna a garantire che i sistemi di IA adottati rispettino i principi fondamentali del trattamento dei dati personali di cui all'art. 5 del GDPR, con particolare riferimento ai principi di liceità, correttezza e trasparenza, limitazione della finalità, minimizzazione dei dati, esattezza, limitazione della conservazione, integrità e riservatezza e responsabilizzazione (accountability). In tale prospettiva, IDRAGEST si impegna altresì a effettuare una Valutazione d'Impatto sulla Protezione dei Dati (DPIA) ai sensi dell'art. 35 del GDPR per i trattamenti ad alto rischio che coinvolgono sistemi di IA, garantendo che la privacy sia integrata nella progettazione dei sistemi fin dalla fase iniziale (privacy by design e privacy by default), in conformità all'art. 25 del GDPR.

Con specifico riferimento ai rischi per la privacy dei dipendenti e dei collaboratori, IDRAGEST riconosce che i sistemi di IA possono essere utilizzati in modo improprio per intensificare dinamiche di controllo e sorveglianza dei lavoratori. La Società si impegna pertanto a non utilizzare sistemi di IA per finalità di monitoraggio invasivo dei dipendenti e dei collaboratori che esulino dai limiti consentiti dalla normativa vigente in materia di tutela della dignità e della riservatezza dei lavoratori, in conformità all'art. 4 della L. 20 maggio 1970, n. 300 (Statuto dei Lavoratori), come modificato dal D.Lgs. 14 settembre 2015, n. 151, e alle Linee Guida del Garante per la Protezione dei Dati Personali in materia di trattamento dei dati dei lavoratori.

4.5. SUPERVISIONE UMANA E RESPONSABILITÀ NELLE DECISIONI

IDRAGEST adotta il principio di supervisione umana significativa (meaningful human oversight) quale presidio fondamentale per garantire che l'utilizzo dell'intelligenza artificiale non comprometta i diritti e gli interessi delle persone. In conformità all'art. 26, par. 1, lett. b), del Regolamento (UE) 2024/1689 (AI Act), IDRAGEST garantisce che i sistemi di IA adottati siano sottoposti a supervisione umana adeguata da parte di personale competente, che gli output del sistema siano verificati prima di qualsiasi utilizzo in contesti rilevanti e che le decisioni di maggiore impatto non siano mai affidate esclusivamente a processi automatizzati.

IL PRINCIPIO DI SUPERVISIONE UMANA SI DECLINA NEI SEGUENTI IMPEGNI OPERATIVI:

(I) RESPONSABILITÀ UMANA IDENTIFICABILE: per ogni sistema di IA adottato da IDRAGEST è identificato un responsabile umano che risponde degli output generati dal sistema e delle decisioni adottate sulla base di tali output, in conformità al principio di accountability di cui all'art. 5, par. 2, del GDPR e all'art. 26 dell'AI Act;

(II) DIRITTO DI CONTESTAZIONE E REVISIONE UMANA: i soggetti interessati dagli output dei sistemi di IA di IDRAGEST hanno il diritto di richiedere una revisione umana delle decisioni che li riguardano, in conformità all'art. 22, par. 3, del GDPR e ai principi di equità e responsabilità dell'AI Act;

(III) TRACCIABILITÀ E SPIEGABILITÀ: IDRAGEST si impegna a garantire che i processi decisionali supportati da sistemi di IA siano tracciabili e spiegabili in termini comprensibili per i soggetti interessati, in conformità al principio di trasparenza dell'AI Act e al diritto degli interessati a ricevere informazioni significative sulla logica dei processi automatizzati ai sensi dell'art. 13, par. 2, lett. f), del GDPR.

4.6. PREVENZIONE DEGLI USI DISTORTI E TUTELA DELLA DIGNITÀ

IDRAGEST riconosce che l'intelligenza artificiale può rappresentare una minaccia per i diritti fondamentali della persona qualora non sia governata con adeguata responsabilità. La Società si impegna pertanto a non utilizzare sistemi di IA per finalità che violino la dignità umana o che integrino pratiche vietate dall'art. 5 del Regolamento (UE) 2024/1689 (AI Act), tra cui:

(i) sistemi di IA che utilizzino tecniche subliminali o manipolative per influenzare il comportamento delle persone in modo da pregiudicarne gli interessi;

(ii) sistemi di IA che sfruttino le vulnerabilità di specifici gruppi di persone, in particolare minori, anziani o persone con disabilità;

(iii) sistemi di IA per la valutazione o la classificazione delle persone fisiche sulla base del loro comportamento sociale o di caratteristiche personali (social scoring);

(iv) sistemi di IA per il riconoscimento biometrico in tempo reale in spazi accessibili al pubblico, salvo le eccezioni tassativamente previste dall'AI Act.

Tali divieti si coordinano con gli obblighi di rispetto del Codice Etico di IDRAGEST e del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001, richiamati all'art. 13 delle Condizioni Generali di Contratto, nonché con il divieto di utilizzo di sistemi di IA generativa senza il previo consenso scritto di IDRAGEST.

4.7. MIGLIORAMENTO CONTINUO E AGGIORNAMENTO DEI PRINCIPI

IDRAGEST si impegna a sottoporre periodicamente a revisione critica i principi e le regole contenuti nel presente articolo, al fine di garantirne la costante adeguatezza rispetto all'evoluzione tecnologica, normativa ed etica nel settore dell'intelligenza artificiale. In particolare, la Società si impegna a recepire tempestivamente le indicazioni del Garante per la Protezione dei Dati Personali, dell'Agenzia per l'Italia Digitale (AgID), dell'Ufficio Europeo per l'IA istituito ai sensi dell'art. 64 del Regolamento (UE) 2024/1689 (AI Act) e di ogni altra autorità competente in materia di intelligenza artificiale, adeguando la presente Policy alle nuove disposizioni normative e alle best practice emergenti nel settore. Ogni aggiornamento dei principi di cui al presente articolo sarà comunicato a tutti i soggetti destinatari della presente Policy con congruo preavviso scritto, in conformità a quanto previsto dall'art. 15.2 della presente Policy, e sarà reso disponibile sulla intranet aziendale di IDRAGEST e sul sito web www.idragest.it.

5 VERSIONI AUTORIZZATE E ACCESSO AL SISTEMA

5.1 VERSIONI AUTORIZZATE E GARANZIE CONTRATTUALI.: IDRAGEST autorizza esclusivamente l'utilizzo delle versioni ChatGPT Business, ChatGPT Enterprise e ChatGPT Edu di OpenAI, nonché degli eventuali ulteriori sistemi di IA Generativa espressamente approvati dal Responsabile IA.

Per le garanzie di sicurezza delle piattaforme autorizzate si rinvia all'art. 8.4 della presente Policy.

Gli Utenti Autorizzati sono tenuti a prendere visione delle policy e delle condizioni d'uso pubblicate dal provider OpenAI, disponibili al seguente indirizzo: **https://openai.com/it-IT/policies/,** invitando, tutti i Destinatari della medesima a prenderne puntuale visione e condivisione. Invero, la presa visione delle suddette policy costituisce parte integrante degli obblighi di utilizzo consapevole e conforme dei sistemi di IA autorizzati.

5.2 VERSIONI NON AUTORIZZATE

È espressamente vietato l'utilizzo delle seguenti versioni e strumenti di IA generativa nell'ambito delle attività lavorative di IDRAGEST:

(i) ChatGPT versione gratuita (consumer) accessibile su chat.openai.com senza account aziendale;

(ii) qualsiasi altro strumento di IA generativa non espressamente autorizzato dal Responsabile IA, indipendentemente dal fatto che sia gratuito o a pagamento;

(iii) modelli di IA installati localmente su dispositivi personali non aziendali;

(iv) API di OpenAI o di altri provider di IA non configurate e approvate dal Responsabile IA.

5.3 ACCESSO E CREDENZIALI

L'accesso a ChatGPT Business/Enterprise/Edu avviene esclusivamente tramite account aziendali nominativi assegnati dal Responsabile IA. È vietata qualsiasi forma di condivisione, cessione o utilizzo promiscuo delle credenziali di accesso.

5.4. PROCEDURA DI AUTORIZZAZIONE

La richiesta di accesso deve essere inoltrata al Responsabile IA tramite apposito modulo interno. L'accesso è subordinato alla previa lettura e accettazione della presente Policy, attestata mediante firma del modulo di accettazione.

6 USI VIETATI E LIMITAZIONI OPERATIVE

6.1 DIVIETO ASSOLUTO DI INSERIMENTI DI DATI RISERVATI

In conformità all'Articolo 5 del Regolamento (UE) 2024/16 è assolutamente vietato inserire nei prompt di ChatGPT le seguenti categorie di informazioni:

(i) dati personali di dipendenti, clienti, fornitori o terzi (nome, cognome, codice fiscale, dati di contatto, dati sanitari, dati bancari), ai sensi degli artt. 5 e 9 del GDPR;

(ii) informazioni confidenziali di Clienti di IDRAGEST, ivi inclusi dati tecnici di progetto, planimetrie, rilievi, relazioni tecniche riservate;

(iii) segreti industriali, know-how proprietario, algoritmi e metodologie di calcolo sviluppati da IDRAGEST, tutelati dal D.Lgs. 10 febbraio 2005, n. 30 (Codice della Proprietà Industriale);

(iv) dati finanziari riservati, offerte commerciali in corso di negoziazione, prezzi unitari non pubblici;

(v) informazioni relative a procedure concorsuali, contenziosi in corso o potenziali, comunicazioni legali riservate;

(vi) credenziali di accesso a sistemi informativi aziendali, chiavi API, password;

(vii) dati relativi a commesse pubbliche soggetti agli obblighi di riservatezza di cui alla L. 13 agosto 2010, n. 136, e al D.Lgs. 31 marzo 2023, n. 36 (Codice dei Contratti Pubblici);

(viii) l'utilizzo di dati aziendali per il fine-tuning o l'addestramento di modelli senza espressa autorizzazione del Responsabile IA e dell'Ufficio Legale;

(ix) l'impiego di sistemi che utilizzano tecniche subliminali o manipolative idonee a distorcere il comportamento di una persona in maniera che essa non possa rendersi conto, in modo tale da causarle o da poter causarle un danno;

(x) l'utilizzo di sistemi per l'inferenza delle emozioni di persone fisiche nell'ambito del luogo di lavoro e degli istituti di istruzione.

6.2 DIVIETO DI UTILIZZO PER DECISIONI AUTOMATIZZATE VINCOLANTI

È vietato utilizzare gli output di ChatGPT come unica base per decisioni aziendali vincolanti in materia di:

(i) selezione e gestione del personale;

(ii) valutazione tecnica di progetti ingegneristici destinati alla presentazione al Cliente o all'autorità pubblica;

(iii) valutazione della conformità normativa di prodotti, servizi o processi;

(iv) decisioni di natura legale o contrattuale come ad esempio assunzioni, licenziamenti e valutazioni tecniche vincolanti.

6.3 DIVIETO DI PRESENTAZIONE DEGLI OUTPUT COME ELABORATI SENZA REVISIONE

È vietato presentare output generati da ChatGPT come elaborati tecnici o professionali propri di IDRAGEST senza previa revisione critica, validazione tecnica e assunzione di responsabilità da parte del professionista firmatario.

6.4 DIVIETO DI UTILIZZO PER FINALITA' CONTRARIE AL CODICE ETICO

È vietato utilizzare ChatGPT per finalità contrarie ai principi di onestà, imparzialità, trasparenza, lealtà e buona fede sanciti dal Codice Etico di IDRAGEST, ivi inclusa la generazione di contenuti ingannevoli, discriminatori o lesivi della reputazione di terzi.

6.5. DIVIETO DI ADDESTRAMENTO NON AUTORIZZATO

È vietato utilizzare dati aziendali, anche anonimizzati, per addestrare, affinare (fine-tuning) o personalizzare modelli di IA senza la preventiva autorizzazione scritta del Responsabile IA.

6.6. PER GARANTIRE LA SICUREZZA DEI DATI È INDISPENSABILE ADOTTARE LE SEGUENTI MISURE:

a) autenticazione a più fattori per accessi dall'esterno;

b) monitoraggio delle intrusioni;

c) backup e ripristino;

d) formazione del personale;

e) algoritmi di autoapprendimento per rilevare e rispondere alle minacce informatiche in tempo reale;

f) protezione da phishing e deepfake.

7 OBBLIGHI DEGLI UTENTI AUTORIZZATI

7.1 OGNI UTENTE AUTORIZZATO E' TENUTO A:

(i) verificare sempre gli output generati da ChatGPT prima di utilizzarli, avendo cura di controllare l'accuratezza fattuale, la correttezza tecnica, la coerenza logica e la conformità normativa delle informazioni prodotte, consapevole che i modelli di IA possono generare informazioni inesatte o non aggiornate (c.d. «allucinazioni»);

(ii) anonimizzare i dati prima di inserirli nei prompt, sostituendo nomi, riferimenti identificativi e dati sensibili con identificatori generici o fittizi;

(iii) conservare traccia (logging) dei prompt inviati e degli output ricevuti per almeno 12 mesi, al fine di garantire la piena ricostruibilità delle operazioni e la conformità ai requisiti di trasparenza dell'AI Act.;

(iv) segnalare tempestivamente al Responsabile IA qualsiasi anomalia, output inappropriato, potenziale violazione della sicurezza, utilizzo non conforme alla presente Policy o uso improprio di sistemi di IA generativa, di cui venga a conoscenza;

(v) partecipare ai programmi di formazione ed aggiornamento organizzati da IDRAGEST sull'utilizzo responsabile degli strumenti di IA generativa;

(vi) non condividere gli output di ChatGPT con soggetti esterni a IDRAGEST senza previa autorizzazione del proprio responsabile competente o del Responsabile IA, qualora tali output contengano informazioni riservate, dati personali, know-how aziendale o contenuti strategici.

8 SICUREZZA DEI DATI, PROTEZIONE DELLE INFORMAZIONI E CYBERSECURITY

8.1. PROTEZIONE DEI DATI PERSONALI E CONFORMITÀ AL GDPR

IDRAGEST S.r.l. adotta misure tecniche, organizzative e di sicurezza adeguate per la protezione dei dati personali e delle informazioni riservate trattate nell'ambito dell'utilizzo dei sistemi di intelligenza

artificiale, in conformità al Regolamento (UE) 2016/679 (GDPR), al D.Lgs. 30 giugno 2003, n. 196 come modificato dal D.Lgs. 10 agosto 2018, n. 101, e al Regolamento (UE) 2024/1689 (AI Act).

Il GDPR stabilisce un quadro normativo organico volto a proteggere i dati personali di clienti, dipendenti e collaboratori. I sistemi di intelligenza artificiale adottati da IDRAGEST devono essere conformi ai principi fondamentali del trattamento di cui all'art. 5 del GDPR e, in particolare, ai seguenti requisiti specifici:

A) TRASPARENZA E INFORMAZIONE: gli interessati devono essere informati in modo chiaro e accessibile sul trattamento dei loro dati da parte di sistemi di IA, ivi inclusi eventuali processi decisionali automatizzati, in conformità agli artt. 13 e 14 del GDPR e all'art. 50 dell'AI Act, coordinandosi con il principio di trasparenza di cui all'art. 4.1 della presente Policy.

B) CONSENSO E LICEITÀ DEL TRATTAMENTO: il trattamento deve basarsi su una base giuridica valida ai sensi dell'art. 6 del GDPR e, per le categorie particolari di dati di cui all'art. 9 del GDPR, su una delle basi giuridiche specificamente previste dal medesimo articolo. Il consenso al trattamento automatizzato e alla profilazione deve essere raccolto in forma separata, specifica, informata e inequivocabile, in conformità all'art. 7 del GDPR.

C) DIRITTI DEGLI INTERESSATI: gli interessati hanno il diritto di accedere ai propri dati (art. 15 GDPR), di rettificarli (art. 16 GDPR), di ottenerne la cancellazione (art. 17 GDPR), di limitarne il trattamento (art. 18 GDPR), di riceverli in formato portabile (art. 20 GDPR), di opporsi al trattamento (art. 21 GDPR) e di non essere sottoposti a decisioni basate esclusivamente su trattamenti automatizzati che producano effetti giuridici significativi (art. 22 GDPR), in conformità al principio di supervisione umana di cui all'art. 4.5 della presente Policy.

D) VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA): per i trattamenti effettuati mediante sistemi di IA che presentano rischi elevati, è obbligatoria la DPIA (Valutazione d'Impatto sulla Protezione dei Dati) ai sensi dell'art. 35 del GDPR, da effettuarsi prima dell'avvio del trattamento e aggiornata periodicamente.

E) PROCESSO DECISIONALE AUTOMATIZZATO E PROFILAZIONE: in conformità all'art. 22 del GDPR, nessuna decisione vincolante che produca effetti giuridici significativi può essere adottata senza adeguata supervisione umana, in conformità al principio di cui all'art. 4.5 della presente Policy e all'art. 26 dell'AI Act.

8.2. OBBLIGHI OPERATIVI DEI DESTINATARI DELLA POLICY IN MATERIA DI PROTEZIONE DEI DATI

I Destinatari della presente Policy — ivi inclusi dipendenti, collaboratori, consulenti e fornitori che operano per conto di IDRAGEST — sono tenuti ad adottare le seguenti misure operative nell'ambito dell'utilizzo di sistemi di intelligenza artificiale:

(a) Definire le finalità del trattamento prima di avviare qualsiasi attività di trattamento dei dati personali mediante sistemi di IA, garantendo che le finalità siano determinate, esplicite e legittime ai sensi dell'art. 5, par. 1, lett. b), del GDPR;

(b) Informare gli interessati sull'utilizzo che si fa della tecnologia di IA nel trattamento dei loro dati, in conformità agli artt. 13 e 14 del GDPR e al principio di trasparenza dell'AI Act;

(c) Raccogliere il consenso al trattamento automatizzato e alla profilazione nei casi in cui tale base giuridica sia necessaria ai sensi degli artt. 6 e 7 del GDPR, garantendo che il consenso sia libero, specifico, informato e inequivocabile;

(d) Determinare la base giuridica del trattamento prima di avviare qualsiasi attività di trattamento dei dati personali mediante sistemi di IA, documentandola nel Registro delle Attività di Trattamento di cui all'art. 30 del GDPR;

(e) Effettuare la DPIA per i trattamenti ad alto rischio che coinvolgono sistemi di IA, in conformità all'art. 35 del GDPR, e consultare preventivamente il Garante per la Protezione dei Dati Personali nei casi previsti dall'art. 36 del GDPR;

(f) Garantire la spiegabilità e la trasparenza algoritmica, fornendo un prospetto compiuto e completo del funzionamento della tecnologia di IA adottata, al fine di individuarne i criteri di ragionamento e gli eventuali bias di partenza (ovvero potenziali distorsioni algoritmiche), in conformità al principio di trasparenza dell'AI Act e alle Linee Guida per un'IA Affidabile dell'High-Level Expert Group on AI della Commissione Europea;

(g) Intervenire tempestivamente in caso di possibili violazioni dei diritti degli interessati rilevate nell'ambito dell'utilizzo di sistemi di IA, adottando le misure correttive necessarie e segnalando l'evento al Responsabile IA di IDRAGEST;

(h) **COMUNICARE E NOTIFICARE I DATA BREACH:** in caso di violazione dei dati personali riconducibile all'utilizzo di sistemi di IA, il Destinatario è tenuto a notificare immediatamente l'evento al Responsabile IA di IDRAGEST, che provvederà alla notifica al Garante per la Protezione dei Dati Personali entro 72 ore ai

sensi dell'art. 33 del GDPR e, ove necessario, alla comunicazione agli interessati ai sensi dell'art. 34 del GDPR;

(i) Implementare sistemi di logging e tracciabilità per i sistemi di IA ad alto rischio, garantendo la registrazione degli accessi, delle operazioni di trattamento e degli output generati, in conformità agli obblighi di accountability di cui all'art. 5, par. 2, del GDPR e agli obblighi di documentazione tecnica previsti dall'AI Act;

(j) Adottare misure di sicurezza, dichiarate dal provider, rafforzate contro attacchi adversarial e tentativi di manipolazione dei sistemi di IA, in conformità all'art. 32 del GDPR, che impone l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio.

8.3. Divieti Specifici in Materia di Protezione dei Dati e Utilizzo dei Sistemi di IA

I Destinatari della presente Policy non possono: **(1)** inserire dati personali identificativi in strumenti di IA esterni non autorizzati, in violazione dell'art. 5, par. 1, lett. c), del GDPR e dell'art. 12 CGC; **(2)** inserire categorie particolari di dati ai sensi dell'art. 9 del GDPR in sistemi di IA non espressamente autorizzati dal Responsabile IA; **(3)** inserire informazioni commerciali riservate in sistemi di IA, in violazione degli artt. 12 e 10 CGC; **(4)** generare contenuti illegali o non etici, tra cui contenuti discriminatori, razzisti, sessisti, diffamatori, violenti o d'odio, in violazione della normativa antidiscriminatoria e del Codice Etico, nonché contenuti che promuovano attività illegali o violino diritti di proprietà intellettuale di terzi, in violazione della L. n. 633/1941 e del D.Lgs. n. 30/2005; **(5)** utilizzare sistemi di IA per aggirare licenze software o riprodurre contenuti protetti senza autorizzazione, in violazione dell'art. 10 CGC; **(6)** inserire segreti industriali, credenziali di accesso, chiavi API o password in sistemi di IA, in violazione del principio di minimizzazione dei dati del GDPR.

8.4. Garanzie di Sicurezza delle Piattaforme IA Autorizzate

Le piattaforme ChatGPT Business, ChatGPT Enterprise e ChatGPT Edu di OpenAI offrono le seguenti garanzie contrattuali di sicurezza: **(i)** cifratura dei dati sia a riposo che in transito, mediante protocolli crittografici conformi agli standard internazionali; **(ii)** controlli di accesso granulari con funzionalità di amministrazione centralizzata degli account aziendali; **(iii)** reperibilità del team di sicurezza OpenAI 24/7/365 per la gestione degli incidenti; **(iv)** programma di Bug Bounty per la segnalazione responsabile delle vulnerabilità. Nonostante tali garanzie, si ribadisce il divieto assoluto di inserire dati riservati o non

necessari in qualsiasi sistema di IA, anche autorizzato, e l'obbligo di anonimizzazione e minimizzazione dei dati prima di qualsiasi inserimento, in conformità all'art. 5, par. 1, lett. c), del GDPR e all'art. 6.1 della presente Policy.

8.5. Conservazione dei Dati (Data Retention)

La conservazione dei dati trattati nell'ambito dell'utilizzo di sistemi di IA da parte di IDRAGEST avviene in conformità ai principi di limitazione della conservazione di cui all'art. 5, par. 1, lett. e), del GDPR, che impone che i dati personali siano conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Con specifico riferimento alle piattaforme ChatGPT Enterprise e ChatGPT Edu, la documentazione ufficiale OpenAI indica che: **(i)** gli amministratori dell'area di lavoro aziendale controllano la durata di conservazione dei dati all'interno della piattaforma; **(ii)** le conversazioni eliminate dagli amministratori vengono rimosse dai sistemi OpenAI entro 30 giorni dalla cancellazione, salvo obblighi di legge che impongano una conservazione più prolungata. IDRAGEST si impegna a configurare le impostazioni di conservazione dei dati nelle piattaforme autorizzate in modo coerente con le proprie politiche di data retention e con gli obblighi normativi applicabili, garantendo che i dati non siano conservati oltre il periodo strettamente necessario alle finalità del trattamento.

I Destinatari della presente Policy sono tenuti a eliminare le conversazioni contenenti informazioni sensibili o riservate immediatamente dopo il loro utilizzo, senza attendere la scadenza del periodo di conservazione automatica della piattaforma. La conservazione di output di sistemi di IA utilizzati in documenti ufficiali di IDRAGEST è disciplinata dall'art. 7 della presente Policy, che impone la conservazione della traccia dei prompt e degli output significativi per un periodo non inferiore a 12 mesi.

8.6. Misure di Sicurezza Informatica e Cybersecurity

IDRAGEST adotta misure di sicurezza, tecniche ed organizzative, adeguate avanzate per proteggere i sistemi di intelligenza artificiale da minacce cibernetiche e garantire la continuità operativa delle proprie attività. La sicurezza informatica dei sistemi di IA è fondamentale per proteggere sia i dati personali di dipendenti e clienti sia le informazioni confidenziali di IDRAGEST, in conformità all'art. 32 del GDPR — che impone l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio — e al D.Lgs. 4 settembre 2024, n. 138, di recepimento della Direttiva (UE)

2022/2555 (NIS2), che introduce obblighi rafforzati di cybersecurity per i soggetti essenziali e importanti operanti in settori critici, ivi incluso il settore delle acque reflue e delle infrastrutture idriche rilevante per le attività di IDRAGEST.

8.6.1. Principali Minacce Cibernetiche ai Sistemi di IA

IDRAGEST identifica le seguenti minacce cibernetiche principali cui sono esposti i sistemi di intelligenza artificiale adottati nell'ambito delle proprie attività:

A) Data Poisoning (avvelenamento dei dati): tecnica di attacco che consiste nella manipolazione dolosa dei dati utilizzati per addestrare i modelli di IA, con l'obiettivo di alterarne il comportamento e compromettere l'accuratezza degli output generati. Il data poisoning può produrre output incompleti o errati e comportare significative incombenze in termini di privacy, sicurezza e danno reputazionale per IDRAGEST e per i suoi clienti. Per mitigare tale rischio, IDRAGEST adotta le seguenti misure: **(i)** implementazione di rigorose pratiche di quality assurance sui dati utilizzati per l'addestramento dei modelli di IA, con verifica dell'affidabilità e dell'integrità delle fonti dei dati di input; **(ii)** adozione di una politica di gestione dei dati robusta, basata su crittografia e protezione del dato; **(iii)** monitoraggio periodico dei sistemi di IA per individuare tempestivamente potenziali attacchi di data poisoning, rilevare anomalie e adottare azioni correttive. Si precisa che IDRAGEST procederà all'addestramento di modelli di IA proprietari esclusivamente qualora ciò si rendesse necessario per futuri sviluppi, nel rispetto delle misure di sicurezza di cui al presente articolo.

B) Adversarial Attacks (attacchi avversariali): tecnica di attacco che consiste nell'ingannare i sistemi di IA manipolando gli input in modo impercettibile per gli esseri umani ma altamente influente per l'algoritmo, con l'obiettivo di indurre il sistema a generare output errati o fuorvianti. Gli attacchi avversariali possono comportare significative incombenze in termini di privacy, sicurezza e danno reputazionale. Per mitigare tale rischio, IDRAGEST adotta le seguenti misure: **(i)** verifica e pulizia sistematica dei dati utilizzati come input nei modelli di IA, al fine di identificare tempestivamente anomalie e adottare azioni correttive; **(ii)** addestramento dei modelli di IA mediante tecniche di adversarial training, che prevedono l'utilizzo di dati volontariamente alterati per aumentare la resilienza del sistema e ridurne la vulnerabilità agli attacchi avversariali; **(iii)** monitoraggio continuo degli output del modello per intervenire tempestivamente in caso di errori, omissioni o alterazioni riconducibili ad attacchi avversariali.

c) Esfiltrazione dei dati: processo non autorizzato mediante il quale informazioni sensibili o riservate vengono sottratte da un sistema informatico o da una rete, con potenziale violazione degli obblighi di riservatezza e degli obblighi di protezione dei dati personali di cui al GDPR. Il rischio di esfiltrazione dei dati è particolarmente rilevante nell'ambito dell'utilizzo di sistemi di IA generativa, in cui dati sensibili potrebbero essere inavvertitamente inseriti nei prompt e trasmessi a server esterni. IDRAGEST mitiga tale rischio attraverso il divieto assoluto di inserimento di dati riservati nei sistemi di IA e attraverso le misure tecniche di sicurezza.

d) Phishing e Deepfake: tecniche di attacco che sfruttano sistemi di IA generativa per creare comunicazioni fraudolente (phishing) o contenuti audiovisivi falsificati (deepfake) al fine di ingannare dipendenti, clienti o partner di IDRAGEST. Tali attacchi possono compromettere la sicurezza dei sistemi informativi aziendali, violare la riservatezza delle informazioni confidenziali e arrecare danni reputazionali significativi. IDRAGEST adotta misure specifiche di formazione del personale per il riconoscimento di tali attacchi e implementa sistemi tecnici di rilevamento e filtraggio.

8.6.2. Misure Tecniche e Organizzative di Cybersecurity

In conformità all'art. 32 del GDPR e al D.Lgs. n. 138/2024 (NIS2), sono adottate le seguenti misure: **(a)** autenticazione a più fattori (MFA) per tutti gli accessi dall'esterno della rete aziendale; **(b)** sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS); **(c)** backup periodici dei dati e delle configurazioni dei sistemi di IA, con procedure di ripristino testate regolarmente; **(d)** formazione periodica del personale in materia di cybersecurity, come disciplinato dall'art. 13; **(e)** sistemi di sicurezza basati su algoritmi di machine learning per il rilevamento e la risposta automatica alle minacce in tempo reale; **(f)** misure tecniche specifiche per il rilevamento e il filtraggio di comunicazioni fraudolente basate su tecnologie di IA generativa.

Ai sensi dell'Articolo 25 del D.Lgs. 138/2024, ogni incidente significativo di natura informatica — ivi inclusi data breach o episodi di esfiltrazione di dati correlati a sistemi di IA — deve essere notificato tempestivamente al CSIRT Italia, oltre che al Responsabile IA e, ove applicabile, al Garante per la Protezione dei Dati Personali entro 72 ore dall'avvenuta conoscenza.

8.7. Coordinamento con le Condizioni Generali di Contratto di IDRAGEST

Le misure di sicurezza e cybersecurity di cui al presente articolo si coordinano con le seguenti disposizioni delle Condizioni Generali di Contratto di IDRAGEST:

(I) ART. 7.1 (FORZA MAGGIORE): gli attacchi informatici di particolare gravità — ivi inclusi attacchi ransomware, DDoS o altre forme di cyberattacco che impediscano oggettivamente la prosecuzione delle attività — possono configurare eventi di forza maggiore ai sensi dell'art. 7.1 delle Condizioni Generali, con conseguente esonero di responsabilità subordinato alla tempestiva comunicazione via PEC all'altra Parte entro 3 giorni dall'evento, ai sensi dell'art. 7.2 delle medesime Condizioni Generali;

(II) ART. 12 (RISERVATEZZA): la violazione delle misure di sicurezza di cui al presente articolo che comporti la divulgazione non autorizzata di Informazioni Confidenziali costituisce violazione degli obblighi di riservatezza di cui all'art. 12 delle Condizioni Generali, con conseguente responsabilità della Parte Ricevente per tutte le violazioni poste in essere dal proprio personale dipendente e da tutti coloro che agiscono in nome e per conto della medesima, ai sensi dell'art. 12.2 delle Condizioni Generali;

(III) ART. 9 (CLAUSOLA RISOLUTIVA ESPRESSA): la violazione degli obblighi di sicurezza e cybersecurity di cui al presente articolo — in particolare il divieto di inserimento di dati riservati in sistemi di IA non autorizzati e gli obblighi di notifica dei data breach — può comportare la risoluzione di diritto del contratto ai sensi dell'art. 1456 c.c., in conformità a quanto previsto dall'art. 9.2, lett. ii) e v), delle Condizioni Generali di Contratto di IDRAGEST;

(IV) ART. 14 (INTELLIGENZA ARTIFICIALE): il Cliente è tenuto ad assistere IDRAGEST nello svolgimento dei propri obblighi di conformità ai sensi del GDPR e dell'AI Act, ai sensi dell'art. 14.2, n. 1, delle Condizioni Generali, ivi inclusi gli obblighi di sicurezza e cybersecurity di cui al presente articolo;

(V) ART. 15 (TRATTAMENTO DEI DATI PERSONALI): ciascuna Parte si impegna a manlevare e tenere indenne l'altra da ogni danno, onere, costo, spesa, contestazione e/o pretesa promossa per la tutela dei dati personali da parte dei soggetti interessati e/o delle competenti autorità, in caso di violazione delle disposizioni vigenti in materia, ai sensi dell'art. 15.1 delle Condizioni Generali di Contratto di IDRAGEST.

8.8. GESTIONE DEGLI INCIDENTI DI SICUREZZA

In caso di incidente di sicurezza informatica che coinvolga sistemi di IA adottati da IDRAGEST, i Destinatari della presente Policy sono tenuti ad attivare immediatamente la seguente procedura di gestione degli incidenti:

(I) Notifica immediata al Responsabile IA di IDRAGEST, con descrizione dell'incidente, della tipologia di dati coinvolti e delle misure di contenimento adottate;

(II) CONTENIMENTO DELL'INCIDENTE: adozione immediata delle misure tecniche necessarie per limitare la propagazione dell'attacco e prevenire ulteriori danni, ivi inclusa la sospensione dell'utilizzo del sistema di IA coinvolto;

(III) Valutazione del rischio per i diritti e le libertà delle persone fisiche interessate, al fine di determinare la necessità di notifica al Garante per la Protezione dei Dati Personali ai sensi dell'art. 33 del GDPR;

(IV) Notifica al Garante entro 72 ore dalla scoperta della violazione, qualora la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 33 del GDPR;

(V) Comunicazione agli interessati, qualora la violazione dei dati personali sia suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, ai sensi dell'art. 34 del GDPR;

(VI) Documentazione dell'incidente nel Registro delle Violazioni dei Dati Personali di cui all'art. 33, par. 5, del GDPR, con indicazione delle misure adottate per rimediare alla violazione e prevenire il ripetersi dell'evento;

(VII) Segnalazione all'Organismo di Vigilanza di IDRAGEST, qualora l'incidente di sicurezza possa configurare un reato presupposto ai sensi del D.Lgs. n. 231/2001, ivi inclusi i reati informatici di cui all'art. 24-bis del medesimo Decreto.

9 CONFORMITÀ ALL'AI ACT - REGOLAMENTO UE 2024/1689

9.1. IDRAGEST adotta la presente Policy in conformità al Regolamento (UE) 2024/1689 (AI Act) e ai relativi principi di governance, trasparenza, sicurezza e supervisione umana dei sistemi di IA. Per il quadro normativo completo dell'AI Act e per il calendario di applicazione progressiva delle sue disposizioni si rinvia agli artt. 3.1.1 e 3.6 della presente Policy. Le piattaforme ChatGPT Business, ChatGPT Enterprise e ChatGPT Edu sono classificate come sistemi di IA per uso generale (GPAI) ai sensi dell'art. 3, par. 1, n. 63, dell'AI Act, soggetti agli obblighi degli artt. 51-56 del Regolamento.

9.2. CHATGPT BUSINESS/ENTERPRISE/EDU È CLASSIFICATO COME SISTEMA DI IA PER USO GENERALE (GPAI) AI SENSI DELL'ART. 3, PAR. 1, N. 63, DELL'AI ACT. IDRAGEST, IN QUALITÀ DI DEPLOYER (OVVERO FI UTILIZZATORE), È TENUTA A:

In conformità all'art. 26 dell'AI Act, IDRAGEST si impegna a: **(i)** utilizzare i sistemi ChatGPT Business/Enterprise/Edu esclusivamente in conformità alle istruzioni d'uso, alle politiche di utilizzo accettabile e alla documentazione tecnica fornita da OpenAI, consultabile al link https://openai.com/it-

IT/policies/; **(ii)** garantire che tutti gli Utenti Autorizzati dispongano di un livello sufficiente di alfabetizzazione e formazione in materia di IA, ai sensi dell'art. 4 dell'AI Act, attraverso i programmi di formazione di cui all'art. 13 della presente Policy; **(iii)** non utilizzare sistemi di IA per finalità contrarie alla legge, ai diritti fondamentali delle persone o alle pratiche vietate dall'AI Act; dall'art. 5 dell'AI Act, come disciplinato dall'art. 4.6 della presente Policy; **(iv)** garantire la supervisione umana significativa degli output, in conformità all'art. 4.5 della presente Policy, senza che alcun output possa essere utilizzato come unica base per decisioni vincolanti ai sensi dell'art. 6.2 della presente Policy; **(v)** sospendere immediatamente l'utilizzo di qualsiasi sistema di IA che presenti rischi per la salute, la sicurezza o i diritti fondamentali, ai sensi dell'art. 26, par. 5, dell'AI Act, attivando la procedura di cui all'art. 8.8 della presente Policy; **(vi)** garantire adeguati livelli di trasparenza, tracciabilità e comprensibilità degli output e dei processi supportati da sistemi di IA, nel rispetto dei diritti degli interessati previsti dall'AI Act e dal GDPR.

9.3. IDRAGEST si impegna a monitorare l'evoluzione della normativa in materia di IA e ad aggiornare la presente Policy in conformità alle disposizioni dell'AI Act man mano che queste diverranno applicabili.

10 PROPRIETÀ INTELLETTUALE DEGLI OUTPUT E DIRITTO D'AUTORE

10.1. Tutti i diritti di proprietà intellettuale sugli output generati da ChatGPT nell'ambito delle attività lavorative di IDRAGEST spettano a IDRAGEST S.r.l., nei limiti di quanto consentito dalla normativa vigente in materia di diritto d'autore e fatti salvi eventuali diritti di terzi.

Gli output generati tramite IA sono tutelabili dal diritto d'autore solo in presenza di un apporto creativo umano significativo, ai sensi dell'Articolo 1 della L. 633/1941. In ogni caso, gli utenti sono tenuti a verificare l'originalità del materiale prodotto, per evitare violazioni dei diritti di proprietà intellettuale di terzi.

È espressamente vietato l'utilizzo di opere protette da copyright di terzi per attività di addestramento (fine-tuning) non autorizzato, nonché qualsiasi forma di Text and Data Mining non conforme all'Articolo 70-quater della L. 633/1941.

10.2. GLI UTENTI AUTORIZZATI RICONOSCONO CHE:

(i) gli output generati da ChatGPT potrebbero non essere tutelabili come opere dell'ingegno ai sensi della L. 22 aprile 1941, n. 633 (Legge sul Diritto d'Autore), in assenza di un apporto creativo umano significativo;

(ii) IDRAGEST non può garantire l'originalità degli output generati da ChatGPT, che potrebbero riprodurre contenuti protetti da diritto d'autore di terzi;

(iii) prima di utilizzare output di ChatGPT in documenti ufficiali, relazioni tecniche o materiali destinati a terzi, l'Utente Autorizzato è tenuto a verificare l'assenza di violazioni di diritti di terzi.

10.3. È vietato presentare output di ChatGPT come elaborati originali di IDRAGEST in contesti in cui la paternità intellettuale sia rilevante (es. partecipazione a gare d'appalto, pubblicazioni scientifiche, deposito di brevetti) senza adeguata disclosure.

11 COORDINAMENTO CON IL MODELLO 231 E IL CODICE ETICO

11.1. L'utilizzo di ChatGPT Business/Enterprise/Edu deve avvenire nel pieno rispetto del Codice Etico e del Modello di Organizzazione, Gestione e Controllo adottato da IDRAGEST ai sensi del D.Lgs. 8 giugno 2001, n. 231.

11.2 E' espressamente vietato utilizzare chatgbt per finalità contrarie alla presente Policy, al Codice Etico, o per che possano integrare un reato presupposto ai sensi del D.Lgs. n. 231/2001. Pertanto, ogni violazione dei citati atti dovrà essere segnalata all'Organismo di Vigilanza di IDRAGEST attraverso i canali di Whistleblowing previsti dal Modello 231

11.3. Qualsiasi violazione della presente Policy che possa integrare un reato presupposto ai sensi del D.Lgs. n. 231/2001 deve essere segnalata all'Organismo di Vigilanza di IDRAGEST attraverso i canali di Whistleblowing previsti dal Modello 231.

12 RESPONSABILE IA E STRUTTURA DI GOVERNANCE

12.1. IDRAGEST DESIGNA UN RESPONSABILE IA QUALE REFERENTE INTERNO PER LA GOVERNANCE DEI SISTEMI IA UTILIZZATI DALLA SOCIETA', ATTRIBUENDOGLI I SEGUENTI COMPITI:

(i) gestione degli account aziendali di ChatGPT Business/Enterprise/Edu e delle autorizzazioni di accesso;

(ii) monitoraggio del rispetto della presente Policy;

(iii) proposta di aggiornamento della Policy in conformità all'evoluzione normativa e tecnologica;

(iv) organizzazione dei programmi di formazione, aggiornamento e sensibilizzazione del personale;

(v) gestione degli incidenti di sicurezza e delle problematiche connessi all'utilizzo di strumenti di IA;

(vi) supporto e coordinamento con l'Organismo di Vigilanza per le questioni relative al Modello 231.

12.2. Il Responsabile IA è nominato con apposita delibera del CDA di IDRAGEST e risponde direttamente al legale rappresentante della società e opera in coordinamento con le funzioni competenti in materia di compliance, privacy, cybersecurity e organizzazione aziendale.

12.3 Il Responsabile IA è il sig. VALERIO MIRABELLA con indirizzo email: valerio.mirabella@idragest.it.

IL RESPONSABILE IA SI RELAZIONA CON:

- Il Responsabile della Protezione dei Dati (DPO), per i profili di tutela della privacy;
- Il responsabile IT/Cybersecurity, per la sicurezza informatica dei sistemi;
- Le Risorse Umane, per gli aspetti di formazione, utilizzo e disciplina del personale;
- L'Organismo di Vigilanza ex D.Lgs. 231/2001, per la prevenzione dei reati presupposto.

13 FORMAZIONE E ALFABETIZZAZIONE IN MATERIA DI IA

13.1 In conformità all'art. 4 del Regolamento (UE) 2024/1689 (AI Act), IDRAGEST garantisce che tutti gli utenti autorizzati dispongano di adeguati livelli di alfabetizzazione e formazione in materia di intelligenza artificiale ("AI literacy"), comunque proporzionati alle funzioni svolte, al livello di responsabilità e ai rischi connessi all'utilizzo dei sistemi di IA.

13.2. A TAL FINE, IDRAGEST ORGANIZZA:

1. Un corso iniziale di formazione obbligatorio per tutti i nuovi utenti autorizzati, da completare prima dell'attivazione dell'accesso a ChatGPT Business/Enterprise/Edu;

2. sessioni di aggiornamento periodiche, con cadenza almeno annuale, su novità normative, best practice e rischi emergenti connessi all'utilizzo di strumenti di IA generativa;

3. comunicazioni interne tempestive in caso di aggiornamenti significativi della presente policy o della normativa applicabile.

13.3. la partecipazione ai programmi di formazione di cui al presente articolo è obbligatoria per tutti gli utenti autorizzati e costituisce condizione per il mantenimento dell'accesso agli strumenti aziendali. Pertanto, la Società può limitare, sospendere o revocare le autorizzazioni di accesso ai sistemi di IA in caso di mancata partecipazione ai programmi formativi obbligatori o di reiterata inosservanza delle disposizioni della presente Policy.

14 SANZIONI E CONSEGUENZE DELLE VIOLAZIONI

14.1. La violazione della presente Policy da parte dei dipendenti di IDRAGEST costituisce inadempimento degli obblighi contrattuali e può comportare l'applicazione di provvedimenti disciplinari previste dal Contratto Collettivo Nazionale di Lavoro applicabile e dal Regolamento Aziendale, proporzionate alla gravità della violazione.

14.2. LA VIOLAZIONE DELLA PRESENTE POLICY DA PARTE DI COLLABORATORI, CONSULENTI E FORNITORI ESTERNI PUÒ COMPORTARE:

(i) la revoca immediata dell'accesso agli strumenti di IA aziendali;

(ii) la risoluzione del contratto ai sensi dell'art. 1456 c.c.;

(iii) il risarcimento dei danni eventualmente subiti da IDRAGEST e direttamente riconducibili alla predetta violazione.

14.3. In caso di violazione che comporti un trattamento illecito di dati personali, IDRAGEST si riserva di agire nelle competenti sedi giudiziarie e di segnalare l'evento al garante per la protezione dei dati personali.

15. AGGIORNAMENTO E REVISIONE DELLA POLICY

15.1 LA PRESENTE POLICY È SOGGETTA A REVISIONE PERIODICA, CON CADENZA ALMENO ANNUALE, OVVERO IN OCCASIONI DI:

(i) modifiche significative della normativa applicabile (AI Act, GDPR, D.Lgs. n. 231/2001);

(ii) aggiornamenti rilevanti delle funzionalità di ChatGPT Business/Enterprise/Edu;

(iii) incidenti di sicurezza o violazioni della Policy che evidenzino la necessità di adeguamenti;

(iv) modifiche organizzative significative di IDRAGEST.

15.2. Le modifiche alla presente Policy sono comunicate a tutti gli Utenti Autorizzati con congruo preavviso scritto a mezzo e-mail aziendale. In caso di modifiche sostanziali, è richiesta la nuova accettazione della Policy da parte di ciascun Utente Autorizzato.

16 DISPOSIZIONI FINALI

16.1. La presente Policy entra in vigore dalla data di adozione indicata in intestazione e si applica a tutti gli Utenti Autorizzati a decorrere dalla medesima data.

16.2. Per quanto non espressamente disciplinato dalla presente Policy, si applicano le disposizioni del Codice Etico di IDRAGEST, del Modello di Organizzazione, Gestione e Controllo ex D.Lgs. n. 231/2001, delle Condizioni Generali di Contratto, del GDPR, del D.Lgs. n. 196/2003 e del Regolamento (UE) 2024/1689 (AI Act).

16.3. Per qualsiasi chiarimento o segnalazione relativa alla presente Policy, gli Utenti Autorizzati possono rivolgersi al Responsabile IA all'indirizzo e-mail indicato all'art. 11.3.

IDRAGEST S.R.L.

IL LEGALE RAPPRESENTANTE

ING. PATERNÒ FRANCESCO