

 GETOPEN Energy Saving Company	CODICE DI CONDOTTA AZIENDALE		
		Rev. 0	25.06.2026
			Pag. 1 di 25

REVISIONE	APPROVAZIONE	NATURA DELLE MODIFICHE
Rev. 0	Determina dell'Amministratore Unico del 25.06.2026	ADOZIONE

CODICE DI CONDOTTA AZIENDALE

Approvato con determina dell'Amministratore Unico del 25.06.2026

GETOPEN SRL

Energy Saving Company

Via Cesare Vivante 9 – 95123 CATANIA

Part. IVA 05012480876 – R.E.A. N. 336696



Sommario

ART. 1 — FINALITÀ, NATURA GIURIDICA E FONTI	5
1.1 Finalità	5
1.2 Natura giuridica	5
1.3 Fonti di riferimento	6
1.4 Gerarchia documentale	6
ART. 2 — DESTINATARI E AMBITO DI APPLICAZIONE	7
2.1 Destinatari interni	7
2.2 Destinatari esterni	7
2.3 Diffusione e conoscibilità	7
ART. 3 — PRINCIPI GENERALI DI CONDOTTA	8
3.1 Legalità	8
3.2 Correttezza e buona fede	8
3.3 Diligenza e responsabilità	8
3.4 Trasparenza e tracciabilità	8
3.5 Riservatezza	8
3.6 Non discriminazione e pari opportunità	8
3.7 Tutela della dignità e della salute	9
ART. 4 — REGOLE GENERALI DI COMPORTAMENTO OPERATIVO	9
4.1 Rispetto delle deleghe e dei poteri	9
4.2 Rispetto delle procedure interne	9
4.3 Uso degli strumenti aziendali	9
4.4 Obbligo di segnalazione	9
4.5 Divieto di aggiramento dei controlli	10
ART. 5 — INTEGRITÀ E PREVENZIONE DELLA CORRUZIONE	10
5.1 Politica di tolleranza zero	10
5.2 Corruzione con la Pubblica Amministrazione	10
5.3 Corruzione tra privati	10
5.4 Falsità e manipolazione documentale	11
5.5 Fondi occulti e pagamenti irregolari	11
5.6 Intermediari e terze parti	11
ART. 6 — OMAGGI, SPESE DI RAPPRESENTANZA, LIBERALITÀ E UTILITÀ	11



6.1 Principio di moderazione e trasparenza	11
6.2 Divieti specifici	11
6.3 Obblighi di segnalazione	12
6.4 Spese di rappresentanza	12
ART. 7 — RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE.....	12
7.1 Principio di esclusività e autorizzazione	12
7.2 Gare, finanziamenti e concessioni	12
7.3 Gestione dei fondi pubblici	12
7.4 Sistemi informatici pubblici	13
7.5 Reazione a richieste illecite	13
ART. 8 — RAPPORTI CON CLIENTI, FORNITORI, PARTNER E TERZI	13
8.1 Criteri di selezione delle controparti	13
8.2 Due diligence sulle controparti	13
8.3 Clausole contrattuali di integrità	13
8.4 Divieti nei rapporti commerciali	14
ART. 9 — CONFLITTO DI INTERESSI	14
9.1 Definizione	14
9.2 Obblighi di dichiarazione	14
9.3 Obbligo di astensione	15
9.4 Uso di informazioni privilegiate	15
ART. 10 — USO ETICO E RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE	15
10.1 Principio generale	15
10.2 Sorveglianza e supervisione umana	15
10.3 Robustezza tecnica e sicurezza	16
10.4 Protezione dei dati e privacy by design	16
10.5 Trasparenza e spiegabilità	16
10.6 Prevenzione di bias e non discriminazione	16
10.7 Sostenibilità ambientale	16
10.8 Accountability e responsabilità	16
10.9 Codici di condotta specifici per l'IA	17
ART. 11 — INTELLIGENZA ARTIFICIALE NEI RAPPORTI DI LAVORO E NELLA GESTIONE DEL PERSONALE	17
11.1 Ambito di applicazione	17



11.2 Obbligo di informazione	17
11.3 Non discriminazione	17
11.4 Supervisione e ricorso.....	17
11.5 Tutela della dignità e della salute mentale.....	18
ART. 12 — PROTEZIONE DEI DATI PERSONALI E GOVERNANCE DELLE INFORMAZIONI	18
12.1 Principi di trattamento	18
12.2 Accesso ai dati.....	18
12.3 Obblighi di sicurezza	18
12.4 Privacy by design e by default	18
12.5 Dati di terzi.....	19
ART. 13 — INFORMAZIONI RISERVATE, KNOW-HOW E TUTELA DEL PATRIMONIO AZIENDALE	19
13.1 Beni da tutelare	19
13.2 Divieti	19
13.3 Obbligo di restituzione	20
ART. 14 — REGISTRAZIONI, DOCUMENTAZIONE E TRACCIABILITÀ	20
14.1 Obbligo di accuratezza	20
14.2 Divieti	20
14.3 Funzione ai fini del Modello 231	20
ART. 15 — SALUTE, SICUREZZA E AMBIENTE	20
15.1 Obblighi fondamentali.....	20
15.2 Formazione obbligatoria.....	21
15.3 Rilevanza ai fini del Modello 231	21
15.4 Tutela ambientale.....	21
ART. 16 — WHISTLEBLOWING, CANALI DI SEGNALAZIONE E DIVIETO DI RITORSIONE	21
16.1 Obbligo di segnalazione e diritto alla tutela.....	21
16.2 Canali di segnalazione.....	21
16.3 Requisiti della segnalazione	22
16.4 Divieto assoluto di ritorsione	22
16.5 Condotte vietate	22
16.6 Rapporto con il Modello 231	23
ART. 17 — ORGANISMO DI VIGILANZA E DOVERE DI COOPERAZIONE.....	23
17.1 Ruolo e funzioni dell'OdV	23



17.2 Obblighi di cooperazione	23
17.3 Divieto di interferenza	24
17.4 Flussi informativi verso l'OdV	24
ART. 18 — FORMAZIONE, DIFFUSIONE E AGGIORNAMENTO DEL CODICE	24
18.1 Piano formativo	24
18.2 Diffusione	24
18.3 Aggiornamento periodico	25
ART. 19 — VIOLAZIONI, PROPORZIONALITÀ E RACCORDO CON IL SISTEMA SANZIONATORIO	25
19.1 Rilevanza disciplinare delle violazioni	25
19.2 Graduazione delle sanzioni per i dipendenti	25
19.3 Misure nei confronti di terzi	26
19.4 Tutele procedurali	26
ART. 20 — ENTRATA IN VIGORE, REVISIONE E DISPOSIZIONI FINALI	26
20.1 Entrata in vigore	26
20.2 Comunicazione ai destinatari	26
20.3 Interpretazione	26

ART. 1 — FINALITÀ, NATURA GIURIDICA E FONTI

1.1 Finalità

Il presente Codice di Condotta Aziendale (di seguito "Codice") è adottato da GetOpen S.r.l. quale strumento operativo volto a orientare i comportamenti di tutti i soggetti che, a qualsiasi titolo, operano in nome, per conto o nell'interesse della Società. Il Codice definisce regole concrete di condotta, integra i principi del Codice Etico e si raccorda con il sistema sanzionatorio previsto dal Codice disciplinare.

1.2 Natura giuridica

Il Codice costituisce parte integrante del Modello di organizzazione, gestione e controllo adottato ai sensi degli artt. 6 e 7 del D.Lgs. 8 giugno 2001, n. 231. La sua osservanza è condizione essenziale affinché il Modello possa dispiegare la propria efficacia esimente



della responsabilità amministrativa dell'ente. In linea con quanto affermato dall'ANAC, il sistema disciplinare previsto nel Modello deve essere aggiornato per tenere conto della disciplina whistleblowing e degli obblighi da essa derivanti.

Come precisato dalla giurisprudenza di legittimità, il codice etico e il codice di comportamento aziendale costituiscono il necessario completamento del Modello 231, in quanto documenti diretti a individuare, in riferimento all'etica e ai valori che ispirano l'impresa, diritti, doveri e responsabilità di tutti coloro che partecipano alla realtà aziendale.

1.3 Fonti di riferimento

IL PRESENTE CODICE È REDATTO IN COERENZA CON:

1. D.Lgs. 8 giugno 2001, n. 231, sulla responsabilità amministrativa delle persone giuridiche;
2. D.Lgs. 10 marzo 2023, n. 24, in materia di whistleblowing e protezione dei segnalanti;
3. L. 6 novembre 2012, n. 190, in materia di prevenzione e repressione della corruzione;
4. Linee Guida ANAC n. 1/2025 in materia di whistleblowing;
5. Regolamento UE 2024/1689 (AI Act);
6. L. 23 settembre 2025, n. 132, in materia di intelligenza artificiale;
7. D.Lgs. 9 aprile 2008, n. 81, in materia di salute e sicurezza;
8. CCNL Metalmeccanica Industria vigente;
9. L. n. 300/1970 (Statuto dei Lavoratori), art. 7;
10. Regolamento UE 2016/679 (GDPR).

1.4 Gerarchia documentale

IL CODICE SI COLLOCA IN UN SISTEMA DOCUMENTALE A TRE LIVELLI:

1. Codice Etico — principi, valori e impegni della Società verso tutti i portatori di interesse;
2. Codice di Condotta Aziendale (il presente documento) — regole operative di comportamento, prescrizioni e divieti specifici;
3. Codice disciplinare — conseguenze sanzionatorie della violazione delle norme.

In caso di antinomia, prevalgono le disposizioni di legge, seguono il Codice Etico, il presente Codice e infine le procedure interne.



ART. 2 — DESTINATARI E AMBITO DI APPLICAZIONE

2.1 Destinatari interni

SONO DESTINATARI DEL PRESENTE CODICE, SENZA DISTINZIONE DI RUOLO O LIVELLO GERARCHICO:

1. l'Amministratore Unico e i componenti degli organi sociali;
2. i dirigenti;
3. i quadri e gli impiegati di ogni livello;
4. gli operai e il personale di produzione;
5. i lavoratori in lavoro agile, trasferta o distacco;
6. i tirocinanti, gli stagisti e i lavoratori interinali.

2.2 Destinatari esterni

IL CODICE SI APPLICA, PER QUANTO COMPATIBILE CON LA NATURA DEL RAPPORTO, ANCHE A:

1. collaboratori autonomi, consulenti, professionisti e agenti;
2. fornitori, appaltatori e subappaltatori;
3. partner commerciali e joint venture;
4. qualsiasi altro soggetto terzo che operi per conto della Società in virtù di un rapporto contrattuale.

I contratti con soggetti terzi devono contenere clausole che ne vincolo il rispetto dei principi del Codice, con previsione espressa della facoltà di risoluzione in caso di accertata violazione degli stessi.

2.3 Diffusione e conoscibilità

LA SOCIETÀ ASSICURA CHE IL PRESENTE CODICE SIA PORTATO A CONOSCENZA DI TUTTI I DESTINATARI MEDIANTE:

1. affissione in luogo accessibile in ciascuna sede aziendale;
2. pubblicazione nella intranet aziendale;
3. invio per posta elettronica a ogni lavoratore, con conferma di ricezione;
4. consegna a ogni nuovo assunto contestualmente alla firma del contratto.

Per i lavoratori in modalità agile o da remoto, la trasmissione avviene esclusivamente in formato digitale, con idonea conferma di avvenuta ricezione, nel rispetto di quanto previsto dall'art. 6 del Codice disciplinare.

L'ignoranza del Codice non costituisce esimente dalla responsabilità disciplinare.



ART. 3 — PRINCIPI GENERALI DI CONDOTTA

3.1 Legalità

Ogni destinatario deve conformare la propria condotta alle leggi, ai regolamenti, alle normative applicabili e alle disposizioni interne della Società. Non è consentito conseguire vantaggi in violazione della legge, anche qualora ciò potesse risultare nell'interesse economico della Società.

3.2 Correttezza e buona fede

I rapporti con colleghi, clienti, fornitori, pubbliche amministrazioni e qualsiasi altra controparte devono ispirarsi ai principi di buona fede, correttezza e lealtà, sia nella fase precontrattuale sia nell'esecuzione dei rapporti giuridici. Ogni dichiarazione resa nell'ambito dell'attività aziendale deve essere veritiera, completa e non fuorviante.

3.3 Diligenza e responsabilità

Il destinatario deve svolgere le proprie mansioni con cura, attenzione e professionalità, nell'ottica di preservare l'integrità dell'organizzazione e tutelare il patrimonio aziendale. La diligenza implica anche l'aggiornamento continuo sulle normative e le procedure applicabili al proprio ruolo.

3.4 Trasparenza e tracciabilità

Ogni operazione avente rilevanza per la Società deve essere documentata, motivata, autorizzata e verificabile. Il principio di tracciabilità si applica tanto alle operazioni finanziarie quanto a quelle organizzative, informatiche e di gestione dei dati.

3.5 Riservatezza

Le informazioni acquisite nell'esercizio delle proprie funzioni devono essere trattate con la massima riservatezza. L'obbligo di riservatezza permane anche dopo la cessazione del rapporto con la Società. Ciò vale sia per le informazioni attinenti alla Società e ai suoi clienti, sia per i dati personali di dipendenti, collaboratori e terzi.

3.6 Non discriminazione e pari opportunità

È vietata qualsiasi forma di discriminazione basata su sesso, età, origini etniche, nazionalità, credo religioso, opinioni politiche, orientamento sessuale, condizioni di disabilità o qualsiasi altra caratteristica personale. I sistemi di IA adottati dalla Società non devono amplificare né introdurre bias discriminatori.



3.7 Tutela della dignità e della salute

È garantito a ogni lavoratore e collaboratore un ambiente lavorativo rispettoso della dignità personale, libero da molestie, intimidazioni, violenza psicologica o fisica. La salute fisica e mentale dei lavoratori è un valore primario da preservare anche nell'organizzazione del lavoro e nell'uso di strumenti digitali.

ART. 4 — REGOLE GENERALI DI COMPORTAMENTO OPERATIVO

4.1 Rispetto delle deleghe e dei poteri

Ogni destinatario deve operare esclusivamente nei limiti dei poteri, delle deleghe e delle procure che gli sono stati attribuiti. È vietato compiere atti che eccedano tali limiti o che possano impegnare la Società in modo non autorizzato.

4.2 Rispetto delle procedure interne

I DESTINATARI SONO TENUTI A OSSERVARE SCRUPOLOSAMENTE:

1. le procedure operative e i protocolli aziendali;
2. le istruzioni impartite dai responsabili gerarchici;
3. gli ordini di servizio e le circolari interne;
4. le policy informatiche, di sicurezza, anticorruzione, privacy e IA;
5. i contratti e le normative applicabili al settore.

4.3 Uso degli strumenti aziendali

I beni, le strumentazioni e i sistemi informatici aziendali devono essere utilizzati esclusivamente per finalità lavorative, con cura e nel rispetto delle policy aziendali vigenti.

È vietato:

1. utilizzare strumenti aziendali per scopi privati in modo non autorizzato;
2. installare software non approvato;
3. accedere a siti o contenuti non pertinenti all'attività lavorativa;
4. consentire l'accesso a terzi non autorizzati ai sistemi informatici della Società.

4.4 Obbligo di segnalazione

Ogni destinatario che venga a conoscenza di comportamenti illeciti, violazioni del presente Codice, del Codice Etico, del Modello 231 o di qualsiasi procedura interna, è tenuto a



segnalarli tempestivamente mediante i canali interni predisposti dalla Società, nel rispetto delle garanzie di riservatezza previste dall'art. 16.

4.5 Divieto di aggiramento dei controlli

È vietato aggirare, disattivare, alterare o rendere inefficaci i sistemi di controllo interno, di sicurezza informatica, di tracciabilità finanziaria o di monitoraggio delle operazioni. Qualsiasi tentativo di neutralizzare i presidi organizzativi del Modello 231 costituisce grave violazione del presente Codice.

ART. 5 — INTEGRITÀ E PREVENZIONE DELLA CORRUZIONE

5.1 Politica di tolleranza zero

GetOpen S.r.l. adotta una politica di tolleranza zero nei confronti di qualsiasi forma di corruzione, pubblica o privata, attiva o passiva. Tale politica discende direttamente dai principi del D.Lgs. 231/2001 e dalla L. 190/2012.

5.2 Corruzione con la Pubblica Amministrazione

È ASSOLUTAMENTE VIETATO:

1. offrire, promettere o dare, direttamente o tramite intermediari, denaro o qualsiasi altra utilità a pubblici ufficiali o incaricati di pubblico servizio, nazionali o stranieri, per influenzare decisioni o comportamenti nell'esercizio delle loro funzioni;
2. ricevere, sollecitare o accettare vantaggi indebiti da soggetti pubblici in cambio di comportamenti favorevoli;
3. esercitare o vantare relazioni con soggetti che rivestono funzioni pubbliche, per far ottenere alla Società o a terzi vantaggi indebiti, configurando l'ipotesi di traffico di influenze illecite ai sensi dell'art. 346-bis c.p..

5.3 Corruzione tra privati

È vietato offrire, promettere o concedere denaro o altra utilità, direttamente o tramite intermediari, a direttori generali, dirigenti, sindaci, liquidatori o dipendenti di imprese private, affinché compiano o omettano atti in violazione dei loro obblighi d'ufficio o di fedeltà, a vantaggio della Società. Tale fattispecie integra il reato di corruzione tra privati ai sensi dell'art. 2635 c.c.. Il divieto si applica simmetricamente anche al ricevere utilità indebite.



5.4 Falsità e manipolazione documentale

È vietato alterare, falsificare o distruggere documenti, registrazioni contabili, bilanci o qualsiasi atto rilevante per la Società o per le pubbliche autorità, al fine di occultare condotte illecite o ottenere vantaggi indebiti.

5.5 Fondi occulti e pagamenti irregolari

È vietata la costituzione o l'utilizzo di fondi occulti, conti correnti non dichiarati, casse nere o qualsiasi altro strumento che consenta l'erogazione di pagamenti al di fuori dei sistemi di controllo aziendale.

5.6 Intermediari e terze parti

Il rischio di corruzione mediata deve essere presidiato attraverso un'adeguata due diligence sugli intermediari e le terze parti che agiscono per conto della Società. I contratti con tali soggetti devono contenere clausole anticorruzione e prevedere la possibilità di risoluzione in caso di accertata violazione.

ART. 6 — OMAGGI, SPESE DI RAPPRESENTANZA, LIBERALITÀ E UTILITÀ

6.1 Principio di moderazione e trasparenza

La Società riconosce che omaggi e cortesie commerciali di modesto valore e uso corrente possono essere lecitamente praticate nell'ambito di consuetudini commerciali consolidate, a condizione che:

1. abbiano un valore modesto, non superiore alle soglie stabilite dalla procedura interna "Omaggi e liberalità";
2. non siano finalizzati a influenzare decisioni della controparte;
3. siano coerenti con la dignità del destinatario e il contesto in cui vengono effettuati;
4. siano debitamente documentati e tracciabili.

6.2 Divieti specifici

È VIETATO:

1. erogare omaggi in denaro contante o equivalenti (carte regalo, buoni, criptovalute);
2. riconoscere utilità in connessione temporale o causale con gare d'appalto, ispezioni, procedimenti autorizzativi, trattative commerciali sensibili o verifiche in corso;
3. ricevere doni o utilità al di fuori dei limiti e delle procedure aziendali;



4. frazionare o suddividere tra più destinatari un valore complessivamente superiore alla soglia consentita.

6.3 Obblighi di segnalazione

Qualsiasi proposta di omaggio, ospitalità o utilità che superi i limiti consentiti — ricevuta o formulata — deve essere comunicata tempestivamente al proprio responsabile e, se del caso, all'Organismo di Vigilanza.

6.4 Spese di rappresentanza

LE SPESE DI OSPITALITÀ, EVENTI E RAPPRESENTANZA DEVONO ESSERE:

1. preventivamente autorizzate secondo le deleghe interne;
2. proporzionate e consone al contesto;
3. documentate con idonea giustificazione e registrazione contabile.

ART. 7 — RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE

7.1 Principio di esclusività e autorizzazione

I rapporti con enti pubblici, autorità regolatorie, ispettori, organismi europei e qualsiasi altro soggetto pubblico devono essere gestiti esclusivamente da soggetti autorizzati dalla Società, nel rispetto delle rispettive deleghe.

7.2 Gare, finanziamenti e concessioni

Nei procedimenti di gara, concessione, finanziamento, accreditamento o autorizzazione, è vietato:

1. presentare documentazione falsa, incompleta o manipolata;
2. omettere informazioni rilevanti che la Società avrebbe l'obbligo di comunicare;
3. esercitare pressioni o influenze indebite sui funzionari competenti;
4. instaurare relazioni personali o informali con i responsabili del procedimento al fine di ottenere trattamenti di favore.

7.3 Gestione dei fondi pubblici

I contributi, i finanziamenti, le agevolazioni fiscali o altri vantaggi ottenuti da soggetti pubblici devono essere utilizzati esclusivamente per le finalità per cui sono stati concessi. È vietata qualsiasi deviazione, distrazione o utilizzo improprio di tali risorse, anche parziale, che potrebbe integrare il reato di indebita percezione di erogazioni pubbliche o truffa aggravata ai danni dello Stato.



7.4 Sistemi informatici pubblici

È vietata qualsiasi condotta che, anche involontariamente, possa alterare, danneggiare o interferire con sistemi informatici o telematici di enti pubblici, registri, banche dati ufficiali o reti di rilevanza pubblica.

7.5 Reazione a richieste illecite

QUALORA UN DESTINATARIO RICEVA, DA PARTE DI UN SOGGETTO PUBBLICO, UNA RICHIESTA ANOMALA, UNA PROPOSTA INDEBITA O UNA PRESSIONE CHE POSSA CONFIGURARE CONDOTTA ILLECITA, DEVE:

1. rifiutare fermamente la richiesta;
2. non lasciare spazio ad ambiguità nel proprio comportamento;
3. segnalare tempestivamente l'accaduto al proprio responsabile e all'Organismo di Vigilanza, documentando i fatti.

ART. 8 — RAPPORTI CON CLIENTI, FORNITORI, PARTNER E TERZI

8.1 Criteri di selezione delle controparti

La selezione di fornitori, clienti, partner commerciali e qualsiasi altra controparte contrattuale deve avvenire secondo criteri oggettivi, verificabili e non discriminatori, tra cui:

1. solidità economica e reputazionale;
2. competenza tecnica e professionale;
3. affidabilità nelle precedenti relazioni commerciali;
4. adesione a principi di sostenibilità e integrità;
5. assenza di precedenti penali o disciplinari rilevanti.

8.2 Due diligence sulle controparti

Per le controparti a più elevato rischio — in ragione del settore, del Paese, del valore contrattuale o della tipologia di prestazione — la Società esegue una procedura di due diligence preventiva che comprende la verifica reputazionale, la valutazione del rischio di corruzione e il monitoraggio continuativo.

8.3 Clausole contrattuali di integrità

I CONTRATTI CON FORNITORI, PARTNER E INTERMEDIARI DEVONO INCLUDERE:

1. clausola di adesione ai principi del Codice Etico e del presente Codice;
2. dichiarazione di assenza di conflitti di interesse;



3. obbligo di rispetto della normativa anticorruzione;
4. clausola di risoluzione espressa in caso di violazione accertata.

Come confermato dalla giurisprudenza, la clausola di risoluzione espressa connessa alla violazione del Codice Etico è valida ed efficace quando chiaramente inserita nel contratto e riferita a prescrizioni specifiche.

8.4 Divieti nei rapporti commerciali

È VIETATO:

1. accettare vantaggi personali in connessione a scelte di acquisto, aggiudicazione o partnership;
2. favorire ingiustificatamente una controparte a detrimento di altre;
3. instaurare rapporti con soggetti di dubbia reputazione, coinvolti in procedimenti per reati gravi o collegati ad attività illecite;
4. concludere contratti con condizioni palesemente squilibrate che nascondano utilità indebite.

ART. 9 — CONFLITTO DI INTERESSI

9.1 Definizione

Sussiste un conflitto di interessi ogni volta che l'interesse personale di un destinatario — diretto o indiretto, anche attraverso familiari, conviventi o soggetti a lui collegati — è tale da poter condizionare, anche solo potenzialmente, l'imparzialità delle sue decisioni nell'esercizio delle funzioni aziendali.

9.2 Obblighi di dichiarazione

I DESTINATARI HANNO L'OBLIGO DI DICHIARARE SENZA RITARDO, AI PROPRI RESPONSABILI E, OVE OPPORTUNO, ALL'ORGANISMO DI VIGILANZA:

1. interessi economici personali, diretti o indiretti, in imprese concorrenti, fornitrici o clienti;
2. rapporti familiari o personali con pubblici ufficiali, partner, clienti o fornitori rilevanti;
3. incarichi professionali o consulenziali esterni potenzialmente incompatibili;
4. situazioni patrimoniali suscettibili di influenzare la propria imparzialità.



9.3 Obbligo di astensione

In presenza di un conflitto di interessi, anche solo potenziale, il destinatario deve astenersi da qualsiasi decisione, negoziazione o atto connesso alla situazione conflittuale, informando il proprio superiore e attendendo le istruzioni del caso.

9.4 Uso di informazioni privilegiate

È vietato utilizzare informazioni riservate acquisite nell'esercizio delle proprie funzioni per perseguire interessi personali o di terzi, comprese operazioni su mercati finanziari.

ART. 10 — USO ETICO E RESPONSABILE DELL'INTELLIGENZA ARTIFICIALE

10.1 Principio generale

GetOpen S.r.l., in ragione della propria attività orientata all'innovazione tecnologica, si impegna a sviluppare, acquistare, configurare e impiegare sistemi di intelligenza artificiale in modo affidabile, trasparente, antropocentrico e responsabile.

La ricerca, lo sviluppo, l'adozione, l'applicazione e l'utilizzo di sistemi di IA avvengono nel rispetto dei diritti fondamentali e delle libertà previste dalla Costituzione, del diritto dell'Unione europea e dei principi di trasparenza, proporzionalità, sicurezza, protezione dei dati personali, riservatezza, accuratezza, non discriminazione, parità dei sessi e sostenibilità.

10.2 Sorveglianza e supervisione umana

I sistemi di IA adottati dalla Società devono essere concepiti e configurati in modo da consentire sempre un adeguato controllo e intervento umano. Le decisioni di rilevanza significativa per individui o per l'organizzazione non possono essere adottate sulla base esclusiva di processi decisionali automatizzati, senza la supervisione di personale competente.

Come stabilito dall'art. 3, co. 3, della L. 132/2025: «*I sistemi e i modelli di intelligenza artificiale per finalità generali devono essere sviluppati e applicati nel rispetto dell'autonomia e del potere decisionale dell'uomo, della prevenzione del danno, della conoscibilità, della trasparenza, della spiegabilità*» .



10.3 Robustezza tecnica e sicurezza

I sistemi di IA devono essere sviluppati e utilizzati in modo da essere resilienti contro rischi, malfunzionamenti e tentativi di alterazione o utilizzo improprio. La sicurezza informatica costituisce una preconditione essenziale lungo tutto il ciclo di vita dei sistemi di IA.

10.4 Protezione dei dati e privacy by design

Lo sviluppo e l'utilizzo di sistemi di IA devono avvenire nel pieno rispetto del GDPR e della normativa nazionale applicabile. I principi di minimizzazione dei dati e di protezione fin dalla progettazione e per impostazione predefinita sono applicabili in ogni fase del ciclo di vita del sistema.

Le misure adottate per garantire il rispetto di tali principi possono includere l'anonimizzazione e la cifratura, nonché l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di IA senza trasmissione tra le parti o copia degli stessi dati grezzi.

10.5 Trasparenza e spiegabilità

I destinatari che interagiscono con sistemi di IA, o che ne siano influenzati, devono essere informati di tale circostanza nelle modalità previste dalla legge. La Società garantisce un'adeguata tracciabilità e spiegabilità dei sistemi e delle decisioni adottate con il loro supporto.

10.6 Prevenzione di bias e non discriminazione

È obbligo di ogni destinatario coinvolto nello sviluppo o nell'impiego di sistemi di IA adottare misure concrete per rilevare, mitigare ed eliminare bias algoritmici suscettibili di produrre effetti discriminatori su persone fisiche.

10.7 Sostenibilità ambientale

Lo sviluppo e l'impiego di sistemi di IA deve tenere conto del relativo impatto ambientale, privilegiando soluzioni efficienti dal punto di vista energetico e coerenti con gli impegni di sostenibilità assunti dalla Società.

10.8 Accountability e responsabilità

PER OGNI SISTEMA DI IA ADOTTATO DALLA SOCIETÀ DEVONO ESSERE INDIVIDUATI CHIARAMENTE:

1. il soggetto responsabile del sistema (owner);
2. i soggetti competenti per la sua supervisione;



3. le procedure di escalation in caso di malfunzionamento o risultati anomali;
4. i meccanismi di audit e aggiornamento periodico.

10.9 Codici di condotta specifici per l'IA

La Società può elaborare e adottare codici di condotta specifici per regolamentare l'uso di sistemi di IA in ambiti particolari (es. gestione del personale, analisi di dati di clienti, progettazione di prodotti), in linea con i meccanismi promossi dalla regolamentazione europea in materia di IA.

ART. 11 — INTELLIGENZA ARTIFICIALE NEI RAPPORTI DI LAVORO E NELLA GESTIONE DEL PERSONALE

11.1 Ambito di applicazione

Il presente articolo si applica ogni volta che la Società utilizzi strumenti automatizzati o sistemi di IA in processi che interessano direttamente i lavoratori, tra cui: selezione del personale, valutazione delle prestazioni, organizzazione del lavoro, monitoraggio delle attività, determinazione di compensi o progressioni di carriera.

11.2 Obbligo di informazione

I lavoratori e i candidati devono essere adeguatamente informati dell'utilizzo di sistemi di IA nei processi che li riguardano, nelle modalità e nei termini previsti dalla normativa vigente. L'informazione deve includere la logica del sistema, il tipo di dati trattati e le modalità di intervento umano previste.

11.3 Non discriminazione

I sistemi di IA utilizzati in ambito lavorativo devono garantire parità di trattamento tra i lavoratori, senza operare distinzioni basate su caratteristiche personali protette. I risultati prodotti da tali sistemi devono essere periodicamente verificati al fine di individuare e correggere eventuali effetti discriminatori.

11.4 Supervisione e ricorso

Le decisioni di rilevanza significativa per il lavoratore non possono essere adottate esclusivamente sulla base di processi automatizzati. Deve essere garantita la possibilità di



revisione da parte di personale competente e, nei casi previsti dalla legge, il diritto del lavoratore di esprimere la propria posizione e di contestare la decisione.

11.5 Tutela della dignità e della salute mentale

L'uso di sistemi di IA nel contesto lavorativo non deve determinare un aumento dello stress, della pressione psicologica o della sorveglianza pervasiva dei lavoratori in modo da lederne la dignità o il benessere.

ART. 12 — PROTEZIONE DEI DATI PERSONALI E GOVERNANCE DELLE INFORMAZIONI

12.1 Principi di trattamento

I dati personali dei dipendenti, collaboratori, clienti, fornitori e di qualsiasi altro interessato devono essere trattati nel rispetto del GDPR e della normativa nazionale applicabile. I principi di liceità, correttezza, trasparenza, limitazione delle finalità, minimizzazione, esattezza, limitazione della conservazione e integrità devono essere sempre rispettati.

12.2 Accesso ai dati

Ogni destinatario accede esclusivamente ai dati personali e alle informazioni aziendali necessari per l'esercizio delle proprie mansioni. L'accesso a dati non pertinenti alle proprie funzioni costituisce violazione delle policy aziendali e del presente Codice.

12.3 Obblighi di sicurezza

I DESTINATARI DEVONO:

- 1.** custodire con diligenza le proprie credenziali di accesso ai sistemi;
- 2.** non divulgare password o dati di autenticazione a terzi;
- 3.** segnalare immediatamente all'ufficio IT o al responsabile competente qualsiasi violazione, accesso non autorizzato, smarrimento di dispositivi o data breach;
- 4.** rispettare le policy aziendali in materia di cifratura, conservazione e cancellazione sicura dei dati.

12.4 Privacy by design e by default

Per i sistemi informatici, le applicazioni e i processi che trattano dati personali — in particolare quelli basati su IA — devono essere integrate fin dalla progettazione misure



tecniche e organizzative adeguate a garantire la protezione dei dati. Per impostazione predefinita, devono essere trattati solo i dati personali necessari per ciascuna specifica finalità.

12.5 Dati di terzi

Le informazioni riservate relative a clienti, fornitori e partner acquisite nell'ambito dell'attività professionale non possono essere comunicate a terzi, né utilizzate per finalità diverse da quelle strettamente connesse alla prestazione lavorativa, pena le conseguenze disciplinari e civili previste.

ART. 13 — INFORMAZIONI RISERVATE, KNOW-HOW E TUTELA DEL PATRIMONIO AZIENDALE

13.1 Beni da tutelare

COSTITUISCONO PATRIMONIO AZIENDALE DA PROTEGGERE:

1. le informazioni riservate di carattere tecnico, commerciale, finanziario, strategico e organizzativo;
2. i software, i codici sorgente, i database, i modelli algoritmici e i sistemi sviluppati o acquisiti dalla Società;
3. i progetti, i brevetti, i marchi, i diritti d'autore e qualsiasi altro asset di proprietà intellettuale;
4. i dati di clienti, fornitori e partner;
5. i dati interni relativi a ricerche, offerte, contratti e strategie commerciali.

13.2 Divieti

È VIETATO:

1. copiare, trasferire, diffondere o rendere accessibili dati o documenti aziendali a soggetti non autorizzati;
2. utilizzare le informazioni aziendali per finalità private o a vantaggio di terzi;
3. pubblicare contenuti, immagini o informazioni della Società sui social media o in qualsiasi canale pubblico senza specifica autorizzazione;
4. rimuovere o cancellare dati in modo non autorizzato;
5. appropriarsi, anche solo temporaneamente, di beni aziendali.



13.3 Obbligo di restituzione

Alla cessazione del rapporto, il destinatario è tenuto a restituire immediatamente tutti i beni, i dispositivi, i documenti e i dati in suo possesso, nonché a cancellare dai propri dispositivi personali qualsiasi informazione aziendale riservata.

ART. 14 — REGISTRAZIONI, DOCUMENTAZIONE E TRACCIABILITÀ

14.1 Obbligo di accuratezza

Ogni registrazione contabile, documento, comunicazione interna o esterna, report, relazione tecnica o atto che abbia rilevanza per la Società deve essere:

1. accurato, veritiero e completo;
2. redatto in conformità alle procedure interne e alle norme applicabili;
3. conservato per il periodo previsto dalla legge e dalle policy aziendali.

14.2 Divieti

È VIETATO:

1. alterare, falsificare, manipolare o distruggere documenti aziendali;
2. creare registrazioni contabili false o fuorvianti;
3. utilizzare causali o descrizioni non corrispondenti alla realtà;
4. omettere la registrazione di operazioni che dovrebbero essere documentate;
5. costituire riserve occulte o operare su conti non ufficiali.

14.3 Funzione ai fini del Modello 231

Il principio di tracciabilità è funzionale all'efficace attuazione del Modello 231, il quale, per dispiegare efficacia esimente, richiede che le operazioni aziendali siano sempre ricostruibili e verificabili da parte dell'Organismo di Vigilanza e dell'autorità giudiziaria. I protocolli decisionali devono essere documentati in modo da rendere riconoscibili le fasi di formazione e di attuazione della decisione.

ART. 15 — SALUTE, SICUREZZA E AMBIENTE

15.1 Obblighi fondamentali

OGNI DESTINATARIO, NELL'AMBITO DELLE PROPRIE COMPETENZE, DEVE:

1. rispettare integralmente le disposizioni del D.Lgs. 81/2008 e le procedure aziendali in materia di salute e sicurezza;



2. utilizzare correttamente i dispositivi di protezione individuale e collettivi;
3. non rimuovere, modificare o eludere i dispositivi di sicurezza;
4. segnalare prontamente al proprio responsabile o al RSPP qualsiasi condizione di pericolo, incidente, quasi-incidente o non conformità.

15.2 Formazione obbligatoria

I destinatari sono tenuti a partecipare a tutti i corsi di formazione e addestramento in materia di salute e sicurezza organizzati dalla Società. Il rifiuto ingiustificato di partecipare costituisce violazione del presente Codice.

15.3 Rilevanza ai fini del Modello 231

Il rispetto delle prescrizioni del D.Lgs. 81/2008 costituisce condizione necessaria affinché il Modello organizzativo possa esplicare efficacia esimente in relazione ai reati di omicidio colposo e lesioni gravi o gravissime commesse in violazione delle norme antinfortunistiche, ai sensi dell'art. 25-septies del D.Lgs. 231/2001.

15.4 Tutela ambientale

I destinatari devono contribuire al raggiungimento degli obiettivi di sostenibilità ambientale della Società, adottando comportamenti responsabili nell'uso delle risorse energetiche e dei materiali, nella gestione dei rifiuti e nella riduzione delle emissioni.

ART. 16 — WHISTLEBLOWING, CANALI DI SEGNALEZIONE E DIVIETO DI RITORSIONE

16.1 Obbligo di segnalazione e diritto alla tutela

I destinatari che vengano a conoscenza, nell'ambito del proprio rapporto lavorativo o professionale, di violazioni del presente Codice, del Codice Etico, del Modello 231 o di qualsiasi disposizione normativa rilevante, sono incoraggiati a segnalarlo attraverso i canali interni predisposti dalla Società, nel rispetto delle disposizioni del D.Lgs. 24/2023.

AI SENSI DEL D.LGS. 24/2023, IL GESTORE DEL CANALE INTERNO DEVE:

«rilasciare alla persona segnalante avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione» e «fornire riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento» .

16.2 Canali di segnalazione

LA SOCIETÀ METTE A DISPOSIZIONE:



1. un canale interno di segnalazione, gestito in modo da garantire la riservatezza dell'identità del segnalante, della persona coinvolta e delle persone menzionate nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione;
2. informazioni sul canale esterno gestito dall'ANAC ai sensi dell'art. 7 del D.Lgs. 24/2023.

Le informazioni sui canali di segnalazione disponibili sono esposte in luoghi visibili in ogni sede aziendale e pubblicate nel sito istituzionale della Società.

16.3 Requisiti della segnalazione

Le segnalazioni devono essere circostanziate, basate su fatti ragionevolmente ritenuti veritieri al momento della segnalazione e formulate in buona fede. Non sono tutelate le segnalazioni manifestamente false, calunniose o diffamatorie.

Come precisato dalla giurisprudenza, la normativa sul whistleblowing tutela il lavoratore da reazioni ritorsive, ma non costituisce un'esimente generalizzata per tutte le violazioni disciplinari che il segnalante abbia commesso: l'applicazione di una sanzione disciplinare per comportamenti illeciti propri del dipendente resta al di fuori della copertura fornita dalla norma.

16.4 Divieto assoluto di ritorsione

È fatto divieto assoluto di porre in essere, nei confronti del segnalante, qualsiasi misura ritorsiva, anche solo tentata o minacciata, tra cui: licenziamento, demansionamento, trasferimento, modifica dell'orario di lavoro, sospensione, note disciplinari, referenze negative, discriminazioni.

Le Linee guida ANAC 2025 precisano che il divieto di ritorsioni deve essere richiamato nei codici di comportamento con rinvio alle esemplificazioni contenute nel D.Lgs. 24/2023 e deve assumere natura di obbligo sanzionabile disciplinarmente.

16.5 Condotte vietate

COSTITUISCE VIOLAZIONE GRAVE DEL PRESENTE CODICE:

1. ostacolare o tentare di ostacolare una segnalazione;
2. rivelare intenzionalmente l'identità del segnalante a soggetti non autorizzati;
3. esercitare o favorire ritorsioni nei confronti del segnalante o di suoi familiari;
4. formulare segnalazioni consapevolmente false o calunniose.



16.6 Rapporto con il Modello 231

Il Modello 231 di GetOpen, ai sensi dell'art. 6, co. 2-bis del D.Lgs. 231/2001, deve prevedere canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare coordinato. Come sottolineato da ANAC, il Modello non ha efficacia esimente della responsabilità amministrativa dell'ente qualora non sia adeguato a tali requisiti.

ART. 17 — ORGANISMO DI VIGILANZA E DOVERE DI COOPERAZIONE

17.1 Ruolo e funzioni dell'OdV

L'Organismo di Vigilanza (OdV) è istituito ai sensi dell'art. 6, co. 1, lett. b) del D.Lgs. 231/2001 e ha il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello 231, nonché di curarne l'aggiornamento.

L'ODV DEVE ESSERE DOTATO DI:

1. autonomi poteri di iniziativa e di controllo;
2. adeguate risorse e competenze professionali;
3. indipendenza rispetto alle funzioni operative.

Come confermato dalla giurisprudenza, le funzioni dell'OdV ricomprendono la vigilanza sul funzionamento e l'osservanza del Modello da parte degli organi sociali, dei dipendenti, dei collaboratori e dei consulenti, nonché la verifica dell'effettiva capacità del Modello di prevenire la commissione dei reati presupposto.

17.2 Obblighi di cooperazione

TUTTI I DESTINATARI SONO TENUTI A:

1. collaborare attivamente con l'OdV, fornendo informazioni veritiere, complete e tempestive su richiesta;
2. consentire l'accesso a documentazione, dati e sistemi pertinenti alle attività di vigilanza;
3. partecipare alle interviste e ai controlli programmati dall'OdV;

segnalare proattivamente all'OdV situazioni di rischio, anomalie, violazioni o carenze organizzative.



17.3 Divieto di interferenza

È vietato interferire, ostacolare o condizionare l'attività dell'OdV, anche solo indirettamente, attraverso pressioni, intimidazioni o omissioni informative. La violazione di tale divieto costituisce una delle più gravi infrazioni previste dal presente Codice.

17.4 Flussi informativi verso l'OdV

Devono essere trasmessi periodicamente all'OdV, secondo le modalità stabilite nel Modello 231:

1. i risultati delle attività di controllo e audit interno;
2. le segnalazioni pervenute tramite i canali whistleblowing;
3. le sanzioni disciplinari irrogate;
4. le modifiche organizzative rilevanti;
5. qualsiasi notizia che possa incidere sull'efficacia del Modello.

ART. 18 — FORMAZIONE, DIFFUSIONE E AGGIORNAMENTO DEL CODICE

18.1 Piano formativo

La Società assicura che tutti i destinatari ricevano una formazione adeguata, periodica e verificabile sui contenuti del presente Codice, del Codice Etico e del Modello 231, nonché sulle normative di riferimento.

LE ATTIVITÀ FORMATIVE DEVONO COMPRENDERE:

1. moduli obbligatori di formazione iniziale per i nuovi assunti e collaboratori
2. sessioni periodiche di aggiornamento per il personale esistente;
3. percorsi specialistici per figure a più elevato rischio (responsabili acquisti, commerciale, HR, IT, ricerca e sviluppo);
4. formazione specifica sul whistleblowing, sulla privacy, sull'uso dell'IA e sulla normativa anticorruzione.

ANAC raccomanda espressamente che la formazione sia sempre affiancata a una corretta informazione da parte degli enti sull'utilizzo dei canali di segnalazione interni ed esterni.

18.2 Diffusione

Il presente Codice è diffuso attraverso tutti i canali descritti all'art. 2.3 e deve essere facilmente accessibile a ogni destinatario in ogni momento.



18.3 Aggiornamento periodico

Il Codice è sottoposto a revisione periodica e deve essere aggiornato tempestivamente in caso di:

1. novità normative rilevanti (es. modifiche al D.Lgs. 231/2001, nuova normativa IA, aggiornamenti GDPR, nuove disposizioni anticorruzione);
2. mutamenti organizzativi significativi;
3. emersione di nuovi rischi o di violazioni che evidenzino lacune nel Codice;

modifiche al Modello 231 o al Codice disciplinare.

L'aggiornamento è deliberato dall'Amministratore Unico, sentito l'OdV.

ART. 19 — VIOLAZIONI, PROPORZIONALITÀ E RACCORDO CON IL SISTEMA SANZIONATORIO

19.1 Rilevanza disciplinare delle violazioni

La violazione del presente Codice costituisce inadempimento agli obblighi nascenti dal rapporto di lavoro o dalla collaborazione professionale e dà luogo all'applicazione delle sanzioni previste dal Codice disciplinare di GetOpen S.r.l. in proporzione alla gravità della condotta.

Il D.Lgs. 231/2001 richiede espressamente che il Modello preveda un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello stesso.

19.2 Graduazione delle sanzioni per i dipendenti

Fermo restando quanto previsto nel Codice disciplinare, la gravità della violazione è valutata tenendo conto di:

1. intenzionalità o colpa grave del comportamento;
2. entità del danno o del pericolo provocato;
3. grado gerarchico e responsabilità del destinatario;
4. eventuale recidiva;
5. circostanze attenuanti o aggravanti;
6. collaborazione prestata nell'accertamento dei fatti.

La giurisprudenza di legittimità ha più volte confermato che il principio di proporzionalità della sanzione implica un giudizio di adeguatezza calibrato sulla gravità della colpa e



sull'intensità della violazione, tenuto conto di ogni circostanza utile a valutarne l'effettivo disvalore ai fini della prosecuzione del rapporto.

19.3 Misure nei confronti di terzi

Per i collaboratori, fornitori e partner, la violazione del Codice può comportare:

1. diffida formale;
2. sospensione del rapporto contrattuale;
3. risoluzione del contratto ai sensi della clausola di integrità ivi inserita;
4. azione di risarcimento del danno.

19.4 Tutele procedurali

Ogni procedimento disciplinare deve rispettare le garanzie previste dall'art. 7 della L. 300/1970 e dal CCNL Metalmeccanica Industria, in particolare:

1. previa contestazione scritta, specifica e tempestiva dell'addebito;
2. diritto del lavoratore di presentare giustificazioni scritte o orali entro 5 giorni;
3. possibilità di farsi assistere da un rappresentante sindacale;
4. irrogazione del provvedimento entro 6 giorni dalla scadenza del termine difensivo.

ART. 20 — ENTRATA IN VIGORE, REVISIONE E DISPOSIZIONI FINALI

20.1 Entrata in vigore

Il presente Codice entra in vigore dalla data di approvazione da parte dell'Amministratore Unico di GetOpen S.r.l. e sostituisce ogni precedente versione.

20.2 Comunicazione ai destinatari

Contestualmente alla sua entrata in vigore, il Codice è portato a conoscenza di tutti i destinatari secondo le modalità previste dall'art. 2.3. Per i nuovi assunti e i nuovi collaboratori, la presa visione e accettazione del Codice costituisce requisito essenziale da assolvere al momento dell'instaurazione del rapporto.

20.3 Interpretazione

Eventuali dubbi interpretativi sull'applicazione del presente Codice possono essere sottoposti all'Organismo di Vigilanza, che fornisce i necessari chiarimenti, garantendo la coerenza sistemica con il Modello 231 e con il Codice Etico.

