Modello di Organizzazione, Gestione e Controllo ai sensi del D.Lgs. 231/2001

PARTE GENERALE

REV.	DATA	APPROVATO	NOTE
01	21 gennaio 2025	Consiglio di amministrazione	

SOMMARIO

DEFINIZIONI **5**

STRUTTURA DEL DOCUMENTO **7**

SEZIONE I **8**

1. IL DECRETO LEGISLATIVO N. 231/2001 ..... **8**

2. I REATI CHE DETERMINANO LA RESPONSABILITÀ AMMINISTRATIVA DELL'ENTE **9**

3. I MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO **11**

4. LE LINEE GUIDA DI CONFINDUSTRIA **11**

SEZIONE II **12**

5. DESCRIZIONE DI QUALITAS INFORMATICA **12**

5.1 Storia e attività di Qualitas Informatica 12
5.2 Codice Etico di Gruppo 12
5.3 Finalità e struttura del Modello Organizzativo 12

6. DESTINATARI **13**

7. ADOZIONE DEL MODELLO ORGANIZZATIVO DA PARTE DI QUALITAS INFORMATICA **14**

7.1 Individuazione dei Processi a Rischio 14
7.2 Individuazione e identificazione delle attività a rischio 15
7.3 Disegno dei presidi organizzativi e procedurali 16

8. DIFFUSIONE, COMUNICAZIONE E FORMAZIONE **17**

8.1 La comunicazione iniziale 17
8.2 La comunicazione relativa ad eventuali modifiche del Modello Organizzativo 18
8.3 La formazione 18

9. ORGANISMO DI VIGILANZA E DI CONTROLLO **19**

9.1 Ruolo dell'Organismo di Vigilanza 19
9.2 Composizione e nomina dell'Organismo di Vigilanza 20
9.3 Cause di (in)eleggibilità, revoca, decadenza e sospensione dell'Organismo di Vigilanza 21
9.4 Atti di verifica dell'efficacia e dell'adeguamento costante del Modello Organizzativo e Piano degli Interventi 22
9.5 Obblighi informativi verso l'Organismo di Vigilanza 23
9.6 Segnalazioni di Violazioni-Whistleblowing 24
9.7 Informazioni dell'Organismo di Vigilanza agli organi sociali 25

10. MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE **25**

SEZIONE III **27**

11. SISTEMA DISCIPLINARE **27**

11.1 Principi Generali 27
11.2 Ambito di applicazione 27

11.3 VIOLAZIONI 27
11.4 CRITERI GENERALI DI IRROGAZIONE DELLE SANZIONI 28
11.5 SANZIONI PER I DIPENDENTI (QUADRI – IMPIEGATI) 28
11.6 SANZIONI PER I DIRIGENTI 30
11.7 SANZIONI PER IL VERTICE AZIENDALE 31
11.8 VIOLAZIONI E SANZIONI PER I SOGGETTI TERZI 31

SEZIONE IV 33

12. PROTOCOLLI 33

Allegato 1 – *Catalogo dei Reati e degli Illeciti Amministrativi*

Allegato 2 – *Codice Etico di Gruppo di Gruppo*

Allegato 3 – *Flussi Informativi all'Organismo di Vigilanza*

DEFINIZIONI

Ai fini del Modello di Organizzazione Gestione e Controllo, ove non diversamente specificato, i termini di seguito elencati hanno il significato per ciascuno di essi di seguito attribuito:

- **Codice Etico di Gruppo**: documento contenente i principi etici del Gruppo Impresoft, cui si ispira la Società nello svolgimento delle proprie attività.
- **Decreto Legislativo:** Decreto Legislativo 8 giugno 2001, n. 231, dal titolo "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", pubblicato nella Gazzetta Ufficiale n. 140 del 19 giugno 2001, nonché le successive modifiche ed integrazioni, ivi compresa la Legge 146/2006 che all'art. 10 ne richiama l'applicazione.
- **Destinatari**: soggetti a cui è rivolto il presente Modello Organizzativo, tenuti alla sua osservanza.
- **Ente (o Società):** persona giuridica o associazione anche priva di personalità giuridica. Nel presente Modello Organizzativo: Qualitas Informatica S.p.A. (di seguito più brevemente anche "***Qualitas Informatica***" o "***Società***").
- **Modello Organizzativo:** Modello di Organizzazione e Gestione adottato da Qualitas Informatica, così come previsto dagli articoli 6 e 7 del Decreto Legislativo, quale complesso organico di principi, regole, disposizioni, schemi organizzativi e connessi compiti e responsabilità, volto a prevenire i reati di cui allo stesso Decreto Legislativo.
- **Organismo di Vigilanza (OdV):** Organismo previsto dall'art. 6 del Decreto Legislativo, avente il compito di vigilare sul funzionamento e sull'osservanza del Modello Organizzativo, nonché di curare l'aggiornamento dello stesso.
- **Principi di Comportamento:** principi generali di comportamento, riportati nella Parte Speciale, a cui i Destinatari devono attenersi nello svolgimento delle attività previste dal Modello Organizzativo.
- **Processi a Rischio:** attività aziendali o fasi delle stesse il cui svolgimento potrebbe dare occasione ai comportamenti illeciti (reati o illeciti amministrativi) di cui al Decreto Legislativo.
- **Protocollo (PT):** specifica procedura per la prevenzione dei reati e degli illeciti amministrativi e per l'individuazione dei soggetti coinvolti nelle fasi a rischio dei processi aziendali.
- **Reati**: reati o illeciti amministrativi che, se commessi, possono comportare la responsabilità amministrativa di Qualitas Informatica.
- **Segnalazione:** comunicazione avente ad oggetto il ragionevole e legittimo sospetto o la consapevolezza di Violazioni.

- **Sistema Disciplinare:** insieme delle misure sanzionatorie nei confronti dei Destinatari che commettono Violazioni.
- **Soggetti Terzi:** Consulenti, Fornitori o altri soggetti aventi rapporti negoziali con Qualitas Informatica.
- **Vertice Aziendale (c.d. Soggetti Apicali):** Presidente del Consiglio di Amministrazione, altri membri del Consiglio di Amministrazione.
- **Violazione:** tutti i comportamenti, gli atti e le omissioni consistenti in condotte illecite rilevanti ai sensi del Decreto Legislativo o nelle inosservanze del Modello Organizzativo.

I termini definiti al singolare si intendono anche al plurale ove il contesto lo richieda e viceversa.

Le definizioni di cui al presente documento valgono altresì ove utilizzate nella Parte Speciale e nei Protocolli.

STRUTTURA DEL DOCUMENTO

Il presente documento ha l'obiettivo di illustrare gli elementi costitutivi del **Modello Organizzativo** di Qualitas Informatica.

Esso si compone di quattro sezioni i cui contenuti sono di seguito sintetizzati:

Sezione I
- è volta ad illustrare i contenuti del Decreto Legislativo e delle successive modifiche ed integrazioni, al fine di fornire a tutti i Destinatari del documento un quadro d'insieme del sistema normativo all'interno del quale si inserisce il Modello Organizzativo della Società

Sezione II
- descrive l'articolazione del Modello Organizzativo e ne definisce i contenuti: descrizione di Nemo Industrie, individuazione delle attività a rischio, modalità di gestione dei flussi finanziari all'interno della Società, caratteristiche e funzionamento dell'Organismo di Vigilanza, flussi informativi, attività di formazione e di informazione e modalità di aggiornamento del Modello Organizzativo stesso.

Sezione III
- riporta il sistema disciplinare da attivare nei confronti dei Destinatari che non osservano le norme comportamentali contenute nel Modello Organizzativo.

Sezione IV
- contiene la Parte Speciale ed i Protocolli che devono essere osservati al fine di eliminare o, almeno, ridurre ad un livello accettabile il rischio di comportamenti integranti uno dei reati la cui commissione può comportare l'applicazione delle sanzioni previste dal Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche ed integrazioni.

Allegati
- **Allegato 1** - Catalogo dei Reati e degli Illeciti Amministrativi
- **Allegato 2** - Codice Etico di Gruppo
- **Allegato 3** - Flussi Informativi all'Organismo di Vigilanza

SEZIONE I

1. IL DECRETO LEGISLATIVO N. 231/2001

Il **Decreto Legislativo 8 giugno 2001, n. 231** ha introdotto nell'ordinamento giuridico italiano un sistema di responsabilità amministrativa degli **Enti.**

L'emanazione del **Decreto Legislativo** si inserisce in un contesto legislativo nazionale di attuazione di obblighi internazionali.

Il testo originario, riferito ad una serie di reati commessi nei confronti della Pubblica Amministrazione, è stato integrato da successivi provvedimenti legislativi che hanno ampliato il novero degli illeciti la cui commissione può comportare la responsabilità amministrativa dell'Ente. Inoltre, la L. 146/06 prevede la responsabilità dell'**Ente** in caso di commissione di determinati reati (c.d. Reati Transnazionali).

La **responsabilità dell'Ente** – analoga alla responsabilità penale – sorge per effetto della commissione, da parte di un soggetto legato da un rapporto funzionale con l'**Ente** stesso, di uno dei **Reati** specificamente previsti dal **Decreto Legislativo.**

La responsabilità dell'**Ente** può sussistere qualora i **Reati** siano commessi **nel suo interesse o a suo vantaggio**, mentre non è configurabile nel caso in cui l'autore degli stessi abbia agito nell'interesse esclusivo proprio o di terzi.

Il rapporto funzionale che lega l'autore del **Reato** alla persona giuridica può essere di rappresentanza, di subordinazione o di collaborazione, nei limiti previsti dal **Decreto Legislativo.**

Qualora l'autore del **Reato** sia una persona fisica che riveste funzioni di rappresentanza, di amministrazione, di direzione o di controllo dell'**Ente** o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché una persona che esercita, anche di fatto, la gestione e il controllo dell'Ente, a carico di quest'ultimo è stabilita una presunzione di responsabilità. Ciò in considerazione del fatto che la persona fisica esprime, rappresenta e realizza la politica gestionale dell'**Ente**.

Non c'è presunzione di responsabilità a carico dell'**Ente** qualora l'autore del **Reato** sia una persona sottoposta alla direzione o alla vigilanza di uno dei soggetti di cui al periodo precedente, sicché, in tal caso il fatto del sottoposto comporta la responsabilità dell'**Ente** solo se risulta che la sua realizzazione è stata resa possibile dall'inosservanza degli obblighi di direzione e vigilanza.

La responsabilità (amministrativa) dell'**Ente** è aggiuntiva alla responsabilità (penale) della persona fisica e non sostitutiva della stessa. Dalla sostanziale autonomia di tale responsabilità discende la circostanza che l'**Ente** è chiamato a rispondere del reato anche quando l'autore del medesimo non sia stato identificato o non sia imputabile, ovvero qualora il reato si estingua per causa diversa dall'amnistia. La responsabilità penale della persona fisica resta regolata dal diritto penale comune.

Il Legislatore ha previsto un **sistema sanzionatorio** che si caratterizza per l'applicazione alla persona giuridica di una sanzione, di norma, pecuniaria.

Unitamente alla sanzione pecuniaria, possono essere applicate, in alcuni casi, anche sanzioni interdittive, quali l'interdizione dall'esercizio dell'attività, la sospensione o la revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito, il divieto di contrattare con la Pubblica Amministrazione, l'esclusione da agevolazioni, finanziamenti, contributi o sussidi, l'eventuale revoca di quelli già concessi, il divieto di pubblicizzare beni o servizi.

Alle suddette sanzioni - pecuniarie ed interdittive - si aggiungono la confisca (sempre disposta con la sentenza di condanna) del prezzo o del profitto del reato (anche "per equivalente") e, in determinati casi, la pubblicazione della sentenza di condanna.

Il Legislatore ha, inoltre, previsto che tali misure interdittive - qualora sussistano gravi indizi di responsabilità dell'**Ente** e vi siano fondati e specifici elementi che facciano ritenere concreto il pericolo della commissione di illeciti della stessa indole - possano essere applicate, su richiesta del Pubblico Ministero, anche in via cautelare, già nella fase delle indagini.

Al verificarsi di specifiche condizioni, il Giudice, in sede di applicazione di una sanzione interdittiva che determinerebbe l'interruzione dell'attività dell'Ente, ha la facoltà di nominare un commissario che vigili sulla prosecuzione dell'attività stessa, per un periodo che corrisponde alla durata della pena interdittiva che sarebbe stata applicata.

Sono sottoposte alla disciplina di cui al **Decreto Legislativo** anche le società estere che operano in Italia, indipendentemente dall'esistenza o meno nel paese di appartenenza di norme che regolino in modo analogo la medesima materia.

2. I REATI CHE DETERMINANO LA RESPONSABILITÀ AMMINISTRATIVA DELL'ENTE

I reati da cui può conseguire la responsabilità amministrativa per l'ente (c.d. "reati presupposto") sono espressamente indicati nel **Decreto Legislativo** ed in taluni provvedimenti normativi che ne hanno allargato la portata:

- **indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture** (art. 24 D.lgs. 231/2001);
- **delitti informatici e trattamento illecito dei dati** (art. 24-*bis* D.lgs. 231/2001);
- **delitti di criminalità organizzata** (art. 24-*ter* D.lgs. 231/2001);
- **peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio** (art. 25 D.lgs. 231/2001);
- **falsità in monete, carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (art. 25-*bis* D.lgs. 231/2001);

- **delitti contro l'industria e il commercio** (art. 25-*bis*.1 D.lgs. 231/2001);
- **reati societari** (art. 25-*ter* D.lgs. 231/2001);
- **delitti con finalità di terrorismo o di eversione dell'ordine democratico** (art. 25-*quater* D.lgs. 231/2001);
- **pratiche di mutilazione degli organi genitali femminili** (art. 25-*quater.*1 D.lgs. 231/2001);
- **reati contro la personalità individuale** (art. 25-*quinquies* D.lgs. 231/2001);
- **abusi di mercato** (art. 25-*sexies* D.lgs. 231/2001);
- **omicidio colposo e lesioni gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute del lavoro** (art. 25-*septies* D.lgs. 231/2001);
- **ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio** (art. 25-*octies* D.lgs. 231/2001);
- **delitti in materia di strumenti di pagamento diversi da contanti** (art. 25-*octies*.1 D.lgs. 231/2001);
- **delitti in materia di violazione del diritto d'autore** (art. 25-*novies* D.lgs. 231/2001);
- **induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (art. 25-*decies* D.lgs. 231/2001);
- **reati ambientali** (art. 25-*undecies* D.lgs. 231/2001);
- **impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25-*duodecies* D.lgs. 231/2001);
- **razzismo e xenofobia** (art. 25-*terdecies* D.lgs. 231/2001);
- **frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati** (art. 25-*quaterdecies* D.lgs. 231/2001);
- **reati tributari** (art*. 25-quinquesdecies* D.lgs. 231/2001*)*;
- **contrabbando** (art. *25-sexiesdecies* D.lgs. n. 231/2001);
- **delitti contro il patrimonio culturale** (art. 25-*septiesdecies* D.lgs. 231/2001);
- **riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici** (art. 25-*duodevicies* D.lgs. 231/2001).

Inoltre, la Legge 146/2006, pur non operando un'ulteriore modifica nel corpo del D.lgs. 231/2001, ha esteso la responsabilità degli enti anche alle ipotesi di commissione dei c.d. *reati transnazionali*.

La descrizione delle singole condotte rilevanti ai fini della legge penale viene rinviata all'**Allegato 1** - *Catalogo dei Reati e degli Illeciti Amministrativi*.

3. I MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

Il Decreto Legislativo prevede per l'Ente una **forma specifica di esonero dalla responsabilità** se:

a) l'organo dirigente ha adottato ed efficacemente attuato "*modelli di organizzazione, di gestione e di controllo*" idonei a prevenire i **Reati**;

b) il compito di vigilare sul funzionamento e l'osservanza dei modelli nonché di curare il loro aggiornamento è stato affidato ad un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo;

c) le persone che hanno commesso il reato hanno agito eludendo fraudolentemente i suddetti modelli di organizzazione, gestione e controllo;

d) non vi è stata omessa o insufficiente vigilanza da parte dell'organismo di cui alla lettera b) che precede.

Il **Modello Organizzativo** è l'insieme di regole, riportate nella Parte Speciale e nei Protocolli, sia di carattere comportamentale («*Principi di Comportamento*»), sia di controllo, il cui rispetto - nello svolgimento di attività nell'ambito dei **Processi a Rischio** - consente di prevenire comportamenti illeciti, scorretti, irregolari.

Il mancato rispetto da parte dei **Destinatari** dei Principi di Comportamento e delle modalità operative presenti nella Parte Speciale e nei Protocolli, del Codice Etico di Gruppo e/o nella *Policy Whistleblowing* è sanzionabile. A tal fine, il Modello Organizzativo si compone anche di un sistema disciplinare, previsto ed illustrato nel presente documento.

4. LE LINEE GUIDA DI CONFINDUSTRIA

Nella predisposizione del presente documento, Qualitas Informatica si è ispirata alle Linee Guida di Confindustria.

Resta inteso che la scelta di non adeguare il Modello Organizzativo ad alcune indicazioni di cui alle Linee Guida di Confindustria, non inficia la validità dello stesso. I Modelli di Organizzazione, Gestione e Controllo, infatti, dovendo essere redatti con riferimento alla realtà concreta di Qualitas Informatica, ben possono discostarsi dalle Linee Guida di Confindustria che, per loro natura, hanno carattere generale.

SEZIONE II

5. DESCRIZIONE DI QUALITAS INFORMATICA

5.1 STORIA E ATTIVITÀ DI QUALITAS INFORMATICA

Qualitas Informatica è un'azienda consolidata nel settore industriale che supporta le imprese manifatturiere, italiane ed estere, nella trasformazione digitale e sostenibile della produzione e della logistica degli strumenti produttivi.

In quest'ottica, fin dal 1986, Qualitas sviluppa il sistema MES NET@PRO, un *software* di gestione che integra strumenti digitali avanzati, in grado di automatizzare i processi produttivi per un controllo intelligente degli impianti.

5.2 CODICE ETICO DI GRUPPO

In **data** 21 gennaio 2025 veniva approvato il Codice Etico di Gruppo (**Allegato 2**) che definisce i valori ai quali Qualitas Informatica si ispira nello svolgimento delle attività.

Il Codice Etico di Gruppo contiene i principi etici e le regole di comportamento che il Vertice Aziendale, i Dipendenti, i Consulenti, i Collaboratori, i Fornitori e tutti coloro che operano in nome o per conto di **Qualitas Informatica** sono tenuti a rispettare e/o condividere.

Le disposizioni del **Modello Organizzativo** sono ispirate dai principi etici e dalle regole di comportamento contenuti nel Codice Etico di Gruppo e sono integrate e compatibili con lo stesso.

5.3 FINALITÀ E STRUTTURA DEL MODELLO ORGANIZZATIVO

L'adozione di un **Modello Organizzativo** in linea con le prescrizioni del **Decreto Legislativo** e in particolare degli articoli 6 e 7, unitamente all'emanazione del Codice Etico di Gruppo, è stata assunta nella convinzione che tale iniziativa possa costituire anche un valido strumento di sensibilizzazione nei confronti dei Destinatari, affinché gli stessi, nell'espletamento delle proprie attività, adottino comportamenti corretti e lineari, tali da prevenire il rischio di commissione dei Reati presupposto.

Più in particolare, il Modello si propone le seguenti finalità:

a) predisporre un **sistema strutturato ed organico di prevenzione e controllo**, finalizzato alla riduzione del rischio di commissione dei reati connessi all'attività aziendale e di prevenzione/contrasto di eventuali comportamenti illeciti;

b) determinare, in tutti coloro che operano in nome e/o per conto di Qualitas Informatica, soprattutto nelle "aree di attività a rischio", la **consapevolezza di poter incorrere**, in caso di **Violazione** delle disposizioni ivi riportate, **in un illecito passibile di sanzioni** eventualmente anche penali, e che può comportare altresì sanzioni in capo a **Qualitas Informatica**;

c) informare i Destinatari che la **Violazione** delle prescrizioni contenute nel Modello al cui rispetto sono tenuti comporterà l'**applicazione di apposite sanzioni e, nei casi più gravi, la risoluzione del rapporto contrattuale**;

d) ribadire che **Qualitas Informatica non tollera comportamenti illeciti**, di qualsiasi tipo ed indipendentemente da qualsiasi finalità, in quanto tali comportamenti (anche nel caso in cui **Qualitas Informatica** fosse apparentemente in condizione di trarne vantaggio) sono comunque contrari ai principi etici cui **Qualitas Informatica** intende attenersi.

Il Modello Organizzativo predisposto da **Qualitas Informatica** è volto a definire un sistema di controllo preventivo, diretto in primo luogo a programmare la formazione e l'attuazione delle decisioni di **Qualitas Informatica** in relazione ai rischi/reati da prevenire e composto in particolare da:

- il Codice Etico di Gruppo, che individua i valori primari cui **Qualitas Informatica** intende conformarsi e fissa quindi le linee di orientamento generali dell'attività sociale;
- un sistema organizzativo aggiornato, formalizzato e chiaro, che garantisca una organica attribuzione dei compiti ed un adeguato livello di segregazione delle funzioni;
- procedure formalizzate ed aventi la finalità di regolamentare lo svolgimento delle attività, in particolare relativamente ai processi a rischio, prevedendo opportuni punti di controllo, nonché la separazione di compiti fra coloro che svolgono fasi o attività cruciali nell'ambito di tali processi;
- una chiara attribuzione dei poteri autorizzativi e di firma, coerente con le responsabilità organizzative e gestionali;
- presidi di controllo, relativi in primo luogo alla potenziale commissione di reati presupposto, in grado di fornire tempestiva segnalazione dell'esistenza e dell'insorgere di situazioni di criticità generale e/o particolare.

6. DESTINATARI

Il presente **Modello Organizzativo** è destinato a:

- vertici della Società (a titolo esemplificativo, Presidente e membri del Consiglio di Amministrazione, etc.);
- dipendenti o altre persone - quale che sia il rapporto che li lega a Qualitas Informatica - sottoposti alla direzione o alla vigilanza dei soggetti di cui sopra.

Il rispetto delle prescrizioni dettate dal **Decreto Legislativo**, così come il rispetto dei principi comportamentali indicati nel **Codice Etico di Gruppo**, è richiesto anche ai Soggetti Terzi che operano per Qualitas Informatica mediante la previsione - laddove possibile - di apposite clausole contrattuali.

7. ADOZIONE DEL MODELLO ORGANIZZATIVO DA PARTE DI QUALITAS INFORMATICA

Qualitas Informatica - nell'ambito del sistema di controllo preventivo già esistente - ha posto in essere le attività necessarie per l'adeguamento di tale sistema di controllo a quanto previsto dal **Decreto Legislativo.**

Qualitas Informatica, con l'adozione del **Modello Organizzativo**, si è posta l'obiettivo di dotarsi di un complesso di Principi di Comportamento e di modalità operative diretti a programmare la formazione e l'attuazione delle decisioni in relazione ai reati da prevenire, nel rispetto del sistema di attribuzione di funzioni e di deleghe di poteri, nonché delle procedure interne.

La Parte Speciale ed i Protocolli, intesi come regole a cui devono attenersi i Destinatari, si aggiungono all'intero complesso organizzativo di **Qualitas Informatica** (organigrammi e sistema di attribuzione di poteri) e sono integrate e compatibili con lo stesso.

Il **Modello Organizzativo** è stato adottato dal Consiglio di Amministrazione di **Qualitas Informatica** in data 21 gennaio 2025.

Le modifiche o le integrazioni del **Modello Organizzativo** devono essere approvate dal Consiglio di Amministrazione.

Per le modifiche non sostanziali il Consiglio di Amministrazione nominerà un soggetto delegato che potrà avvalersi del parere dell'**Organismo di Vigilanza**. Tali modifiche verranno comunicate al Consiglio di Amministrazione e da questo ratificate o eventualmente integrate o modificate nella prima adunanza utile. La pendenza della ratifica non priva di efficacia le modifiche nel frattempo adottate.

7.1 INDIVIDUAZIONE DEI PROCESSI A RISCHIO

L'art. 6 comma 2 lett. a) del Decreto Legislativo prevede espressamente che il Modello Organizzativo debba "*individuare le attività nel cui ambito possono essere commessi reati*". Pertanto, Qualitas Informatica ha provveduto ad analizzare le attività aziendali, i processi di formazione e attuazione delle decisioni all'interno delle singole aree aziendali nonché i sistemi di controllo interno.

In particolare, nell'ambito delle suddette attività, Qualitas Informatica con il supporto di Consulenti esterni, ha provveduto a:

a) individuare le attività nel cui ambito potrebbero essere astrattamente commessi i Reati;

b) analizzare i rischi potenziali di illeciti nonché le eventuali modalità di commissione degli stessi;

c) individuare i soggetti e le funzioni aziendali interessati;

d) definire e, all'occorrenza adeguare, il sistema dei controlli interni.

7.2 INDIVIDUAZIONE E IDENTIFICAZIONE DELLE ATTIVITÀ A RISCHIO

Al temine delle verifiche di cui al precedente paragrafo 7.1, Qualitas Informatica ha individuato le attività aziendali o le fasi delle stesse nel cui ambito possono essere astrattamente commessi Reati e/o Illeciti Amministrativi (di seguito i "**Processi a Rischio**").

Al fine di individuare i Processi a Rischio, Qualitas Informatica - con il supporto di Consulenti esterni - ha posto in essere le seguenti attività:

a) disamina della documentazione ufficiale di Qualitas Informatica;

b) mappatura di dettaglio dell'operatività aziendale, articolata sulla base delle unità organizzative di Qualitas Informatica e svolta per il tramite di interviste e questionari di rilevazione;

c) analisi dettagliata di ciascuna singola attività, volta a verificare i precisi contenuti, le concrete modalità operative, la ripartizione delle competenze, nonché la sussistenza o insussistenza di ciascuna delle ipotesi di reato indicate dal Decreto Legislativo.

Specificatamente i **Processi a Rischio** nel cui ambito possono essere astrattamente commessi **Reati**, sono di seguito riportati:

- *acquisto di beni, servizi e consulenze;*
- *adempimenti in materia di salute e sicurezza nei luoghi di lavoro;*
- *adempimenti societari, interventi sul capitale sociale ed operazioni straordinarie;*
- *gestione degli adempimenti fiscali;*
- *gestione del credito e del contenzioso;*
- *gestione dei rapporti con Enti di Certificazione;*
- *gestione dei rapporti con la Pubblica Amministrazione;*
- *gestione del sistema ambientale;*
- *gestione del sistema informativo;*
- *gestione delle attività commerciali e del marketing;*
- *gestione delle note spese e spese di rappresentanza;*
- *gestione di finanziamenti, sovvenzioni o contributi e concessioni o autorizzazioni;*
- *gestione dei flussi finanziari e monetari e adempimenti amministrativo – contabili;*
- *gestione di marchi e brevetti;*
- *rapporti Intercompany;*
- *predisposizione del bilancio d'esercizio;*
- *ricerca, sviluppo e produzione;*
- *selezione, assunzione e gestione del personale.*

Nell'attuale versione del **Modello Organizzativo** risultano individuate come **Processi a Rischio** in relazione al **Decreto Legislativo**, e conseguentemente regolamentate al fine

della prevenzione della commissione di **Reati**, le aree di attività riferite alle seguenti categorie di reati presupposto:

- **reati commessi nei rapporti con la Pubblica Amministrazione** (artt. 24 e 25);
- **delitti informatici e trattamento illecito di dati** (art. 24-*bis*);
- **delitti di criminalità organizzata** (art. 24-*ter*);
- **falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento** (art. 25-*bis*);
- **delitti contro l'industria e il commercio** (art. 25-*bis*.1);
- **reati societari** (art. 25-*ter*);
- **delitti contro la personalità individuale** *(*art. 25-*quinquies);*
- **omicidio colposo e lesioni colpose gravi o gravissime commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute del lavoro** (art. 25-*septies*);
- **ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, nonché autoriciclaggio** (art. 25-*octies*);
- **delitti in materia di strumenti di pagamento diversi dai contanti** (art. 25-*octies*.1);
- **Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria** (Art. 25-*decies*);
- **reati ambientali** (art. 25-*undecies*);
- **reato di impiego di cittadini di paesi terzi il cui soggiorno è irregolare** (art. 25-*duodecies*);
- **reati tributari** (art. 25-*quinquiesdecies*).

Qualitas Informatica si impegna a svolgere un continuo monitoraggio sulla propria attività, sia in relazione ai reati sopra elencati, sia in relazione a possibili modifiche ed integrazioni del **Decreto Legislativo.**

7.3 DISEGNO DEI PRESIDI ORGANIZZATIVI E PROCEDURALI

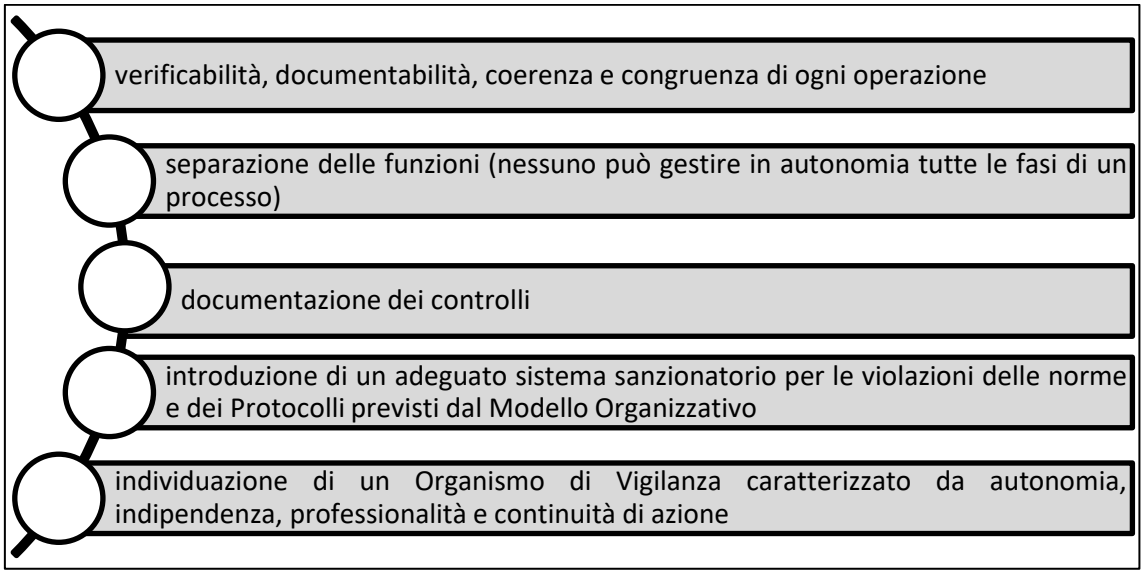
Ai sensi di quanto disposto dall'art. 6, comma 2, del Decreto, il **Modello Organizzativo** deve, tra l'altro, «*prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire*».

La menzionata disposizione evidenzia la necessità di istituire - ovvero migliorare ove esistenti - appositi meccanismi di procedimentalizzazione della gestione e delle decisioni, al fine di rendere documentate e verificabili le varie fasi di ciascun processo aziendale.

Appare dunque evidente che l'insieme di strutture organizzative, attività e regole operative applicabili - su indicazione del *management* - in ambito aziendale deve essere

preordinato a tale specifico obiettivo, con l'intento di garantire, con ragionevole certezza, il raggiungimento delle finalità rientranti in un adeguato ed efficiente sistema di monitoraggio dei rischi, ivi incluso quello di incorrere nelle sanzioni previste dal **Decreto Legislativo**.

L'impianto organizzativo in essere è ispirato ai seguenti principi:



8. DIFFUSIONE, COMUNICAZIONE E FORMAZIONE

L'adeguata formazione e la costante/periodica informazione del personale in ordine ai principi e alle prescrizioni contenute nel **Modello Organizzativo** rappresentano fattori di grande importanza per la corretta ed efficace attuazione del sistema di prevenzione aziendale.

I **Destinatari** sono tenuti ad avere piena conoscenza degli obiettivi di correttezza e trasparenza che si intendono perseguire con il **Modello Organizzativo** e delle modalità attraverso le quali **Qualitas Informatica** ha inteso perseguirli, approntando un adeguato sistema di procedure e controlli.

8.1 LA COMUNICAZIONE INIZIALE

L'adozione del presente **Modello Organizzativo** con i relativi allegati e della *Policy Whistleblowing* è comunicata ai **Destinatari** mediante consegna di copia dello stesso (in formato cartaceo e/o elettronico) che dovrà essere corredata da sottoscrizione di avvenuta ricezione e attraverso l'affissione del documento in luogo accessibile a tutti i **Destinatari**. Inoltre, Qualitas Informatica curerà la pubblicazione del Modello sulla *intranet* aziendale.

Ai nuovi assunti sarà data comunicazione dell'adozione del **Modello Organizzativo** mediante consegna di una copia dello stesso, del **Codice Etico di Gruppo** (in formato cartaceo e/o elettronico) e della *Policy Whistleblowing*.

8.2 LA COMUNICAZIONE RELATIVA AD EVENTUALI MODIFICHE DEL MODELLO ORGANIZZATIVO

Ogni modifica del Modello Organizzativo deve essere comunicata ai **Destinatari**, con illustrazione delle modifiche stesse, mediante meccanismi - anche informatici - atti a comprovarne l'effettiva e consapevole ricezione della comunicazione.

8.3 LA FORMAZIONE

L'attività di formazione finalizzata a diffondere la conoscenza della normativa di cui al **Decreto Legislativo** è differenziata, nei contenuti e nelle modalità di erogazione, in funzione della qualifica dei Destinatari, del livello di rischio dell'area in cui operano e dell'avere o meno funzioni di rappresentanza di **Qualitas Informatica**.

In particolare, il livello di formazione e di informazione del personale di **Qualitas Informatica** avrà un maggior grado di approfondimento con riguardo a coloro che operano nelle aree di attività a rischio.

Rientrano nella formazione, oltre a corsi specifici, anche il ricorso a strumenti di divulgazione, quali, a titolo esemplificativo, occasionali e-mail di aggiornamento o note informative interne.

In ogni caso, successivamente alla formale adozione del **Modello Organizzativo** da parte del Consiglio di Amministrazione, sarà tenuto un corso introduttivo generale finalizzato ad illustrare il quadro normativo di riferimento, i principi di riferimento del Modello Organizzativo, gli obblighi informativi e le regole comportamentali da seguire nelle aree a rischio.

Il programma di formazione potrà essere realizzato con modalità che permettano, tra l'altro, di aggiornare tutti **Destinatari** in merito alle novità, alle integrazioni della normativa e del **Modello Organizzativo**.

La partecipazione obbligatoria ai momenti formativi sarà formalizzata attraverso la richiesta, anche eventualmente in modalità elettronica, della firma di presenza.

Nell'ambito delle proprie attribuzioni, l'**OdV** potrà prevedere specifici controlli volti a verificare la qualità del contenuto dei programmi di formazione e l'effettiva efficacia della formazione erogata.

La mancata partecipazione senza giustificato motivo potrà essere valutata da **Qualitas Informatica** quale violazione del **Modello Organizzativo**.

Qualitas Informatica promuove la conoscenza e l'osservanza del **Modello Organizzativo,** del **Codice Etico di Gruppo** e della *Policy Whistleblowing* anche tra i Collaboratori Esterni e gli altri soggetti terzi individuati dall'Organismo di Vigilanza. La Parte Generale del **Modello Organizzativo** e la *Policy Whistleblowing* vengono portati a conoscenza dei **Soggetti Terzi** mediante pubblicazione sul sito internet della **Società**.

A questi saranno pertanto fornite apposite informative sui principi, le politiche e le procedure che **Qualitas Informatica** ha adottato sulla base del presente Modello,

nonché i testi delle clausole contrattuali che, coerentemente ai principi, alle politiche e ai Protocolli contenuti nel **Modello Organizzativo** nonché nel Codice Etico di Gruppo, saranno adottate da Qualitas Informatica.

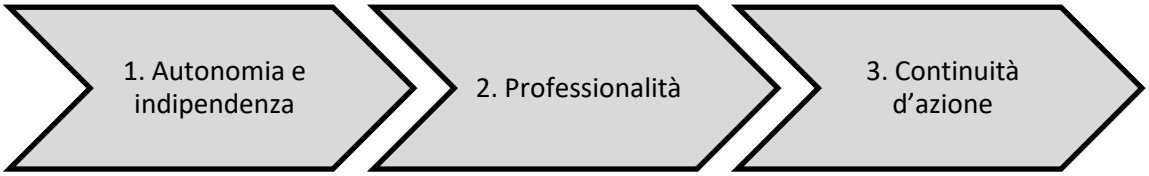
9. ORGANISMO DI VIGILANZA E DI CONTROLLO

9.1 RUOLO DELL'ORGANISMO DI VIGILANZA

Il **Consiglio di Amministrazione** di **Qualitas Informatica**, in attuazione di quanto previsto dal Decreto Legislativo, ha istituito **l'Organismo di Vigilanza e di Controllo (OdV)**, al quale è affidato il compito di **vigilare sul funzionamento e sull'osservanza del Modello Organizzativo**, nonché di **curarne l'aggiornamento**. Sono pertanto di competenza dell'**Organismo di Vigilanza** di **Qualitas Informatica** le attività di vigilanza e controllo previste dal **Modello Organizzativo.**

La nomina dell'OdV, nonché l'eventuale revoca (per giusta causa), sono di competenza del Consiglio di Amministrazione. L'OdV riporta direttamente al **Consiglio di Amministrazione.**

Secondo le disposizioni del Decreto (artt. 6 e 7) e le indicazioni contenute nella Relazione di accompagnamento al Decreto Legislativo, le caratteristiche dell'OdV debbono essere:



1. Autonomia e indipendenza

I requisiti di autonomia e indipendenza garantiscono l'effettivo adempimento dei compiti e delle funzioni assegnate all'OdV. A tal fine è necessario che l'OdV non sia direttamente coinvolto nelle attività gestionali che costituiscono l'oggetto della sua attività di controllo né sia gerarchicamente sottoposto a quanti effettuino dette attività.

Tali requisiti si possono ottenere garantendo all'OdV la più elevata indipendenza gerarchica, prevedendo un'attività di *reporting* al Vertice Aziendale, ovvero all'Amministratore Delegato ed agli altri membri del Consiglio di Amministrazione.

2. Professionalità

L'OdV deve possedere competenze tecnico-professionali adeguate alle funzioni che è chiamato a svolgere. Tali caratteristiche, unite all'indipendenza, garantiscono l'obiettività di giudizio.

3. Continuità d'azione

L'OdV deve:

1 lavorare costantemente sulla vigilanza del Modello Organizzativo con i necessari poteri d'indagine, anche con il supporto di Consulenti esterni;

2 curare l'attuazione del Modello Organizzativo e assicurarne il costante aggiornamento;

3 non svolgere mansioni operative che possano condizionare la visione d'insieme delle attività aziendali che ad esso si richiede.

9.2 COMPOSIZIONE E NOMINA DELL'ORGANISMO DI VIGILANZA

Qualitas Informatica si è orientata nella scelta di un organismo monosoggettivo. Il Consiglio di Amministrazione ottiene, in sede di nomina, l'evidenza circa i requisiti di indipendenza, professionalità nonché i requisiti di onorabilità di cui all'art. 109 del D. Lgs. 1° settembre 1993, n. 385 (*"Requisiti di professionalità e di onorabilità degli esponenti aziendali"*).

L'OdV resta in carica per il periodo definito dal Consiglio di Amministrazione nell'atto di nomina. La sua sostituzione prima della scadenza del mandato può avvenire solo per giusta causa o giustificato motivo, intendendosi per tali, a titolo esemplificativo:

- la volontaria rinuncia da parte dell'OdV;
- la sopravvenuta incapacità per cause naturali;
- il venire meno dei requisiti di onorabilità;
- la mancata comunicazione al Consiglio di Amministrazione del verificarsi di una causa di decadenza di cui al successivo paragrafo 9.3;
- il verificarsi di una delle cause di sospensione o revoca di cui al successivo paragrafo 9.3.

Il Consiglio di Amministrazione di **Qualitas Informatica** stabilisce, per l'intera durata della carica, il compenso annuo spettante all'**Organismo di Vigilanza.**

Nei casi di decadenza, sospensione e revoca di un componente dell'**Organismo di Vigilanza**, il Consiglio di Amministrazione provvede a reintegrane la composizione; il componente di nuova nomina resta in carica per l'intera durata del mandato degli altri componenti.

Per tutti gli altri aspetti operativi, l'**OdV** provvederà ad autoregolamentarsi attraverso uno specifico Regolamento, corredato da norme volte a garantirne il miglior funzionamento. L'adozione di tale regolamento è portata a conoscenza del Consiglio di Amministrazione alla prima seduta utile.

9.3 CAUSE DI (IN)ELEGGIBILITÀ, REVOCA, DECADENZA E SOSPENSIONE DELL'ORGANISMO DI VIGILANZA

Per quanto concerne i requisiti di onorabilità, non possono assumere il ruolo di membri dell'**Organismo di Vigilanza** coloro che si trovino nelle condizioni previste dall'art. 2382 c.c. «*Cause di ineleggibilità e di decadenza*».

Al fine di consentire la valutazione da parte del Consiglio di Amministrazione in merito alla sussistenza o meno di motivi di incompatibilità con la funzione o di conflitto di interesse, l'**OdV** deve comunicare in sede di esame della proposta di nomina:

- conflitti di interesse, anche potenziali, con **Qualitas Informatica**;
- titolarità, diretta o indiretta, di partecipazioni rilevanti per **Qualitas Informatica** ai sensi dell'articolo 2359 c.c.;
- funzioni di amministrazione con deleghe o incarichi esecutivi presso **Qualitas Informatica**;
- pendenze, in Italia o all'estero, di procedimenti penali ovvero condanne, anche non passate in giudicato, o applicazione della pena su richiesta delle parti («*patteggiamento*»), fatti salvi gli effetti della riabilitazione o dell'estinzione del reato.

Sarà cura dell'**OdV** comunicare tempestivamente qualsiasi variazione dovesse intervenire nel corso del mandato.

Compete al Consiglio di Amministrazione, ricevuta tale comunicazione, la valutazione in merito ai requisiti di onorabilità e di compatibilità.

Revoca

Il Consiglio di Amministrazione di **Qualitas Informatica** può revocare l'**OdV** nel caso in cui si verifichino rilevanti inadempimenti rispetto al mandato conferito, in ordine ai compiti indicati nel **Modello Organizzativo**; per ipotesi di violazione degli obblighi di cui al Regolamento dell'**OdV**, nonché quando il Consiglio di Amministrazione venga a conoscenza delle predette cause di ineleggibilità, anteriori alla nomina dell'**OdV** e non indicate nell'autocertificazione; quando intervengano le cause di decadenza di seguito specificate.

Decadenza

L'**Organismo di Vigilanza** decade dalla carica nel momento in cui, successivamente alla sua nomina:

- si trovi in una delle situazioni contemplate nell'art. 2382 c.c. «*Cause di ineleggibilità e di decadenza*»;
- non siano più presenti i requisiti di onorabilità.

Sospensione

Costituiscono cause di sospensione dalla funzione di **Organismo di Vigilanza**:

- l'applicazione di una misura cautelare personale;
- l'applicazione provvisoria di una delle misure di prevenzione previste dall'art. 10, comma 3, della legge 31 maggio 1965, n. 575 «*Disposizioni contro la mafia*», come sostituito dall'articolo 3 della legge 19 marzo 1990, n. 55 e s.m.i.

9.4 ATTI DI VERIFICA DELL'EFFICACIA E DELL'ADEGUAMENTO COSTANTE DEL MODELLO ORGANIZZATIVO E PIANO DEGLI INTERVENTI

L'**OdV**, coordinandosi con i responsabili delle unità organizzative di volta in volta interessate, deve verificare periodicamente l'efficacia e l'idoneità del **Modello Organizzativo** a prevenire la commissione degli illeciti di cui al **Decreto Legislativo**. In particolare, sono previste:

1 **verifiche su singoli atti.** A tal fine procederà periodicamente ad una verifica degli atti e dei contratti relativi ai processi a rischio, secondo modalità dallo stesso individuate;

2 **verifica della Parte Speciale e dei Protocolli.** A tal fine procederà periodicamente ad una verifica dell'efficacia e dell'attuazione della Parte Speciale e dei Protocolli del presente Modello Organizzativo;

3 **verifiche del livello di conoscenza** del Modello Organizzativo anche attraverso l'analisi delle richieste di chiarimenti o delle segnalazioni pervenute;

4 **aggiornamento periodico** dell'attività di *Risk Assessment* finalizzata a rivedere la mappa delle attività potenzialmente a rischio, in particolare in presenza di modifiche dell'organizzazione ovvero del business di Qualitas Informatica, così come in caso di integrazioni o modifiche del Decreto Legislativo.

Ai fini di un programmato esercizio dei poteri di vigilanza assegnati, l'**OdV** presenta annualmente al Consiglio di Amministrazione il proprio **Piano di Intervento**, informandolo circa le attività che prevede di svolgere e le aree che saranno oggetto di verifiche. L'**Organismo di Vigilanza** può comunque effettuare, nell'ambito delle attività aziendali sensibili e qualora lo ritenga necessario ai fini dell'espletamento delle proprie funzioni, controlli non previsti nel Piano di Intervento (cosiddetti "controlli a sorpresa").

Nell'attuazione del Piano degli Interventi, l'**OdV** adotta procedure utili allo svolgimento dell'attività di vigilanza e di controllo, che saranno comunicate alle funzioni interessate, e può istituire gruppi di lavoro su particolari tematiche. In caso di circostanze particolari (ad esempio, emersione di precedenti **Violazioni** o elevato turnover), l'**OdV** avrà cura di applicare sistematiche procedure di ricerca e identificazione dei rischi oggetto di analisi.

In particolare, può richiedere di consultare la documentazione inerente all'attività svolta da singoli Uffici o singole Unità Organizzative e dai soggetti preposti ai processi a rischio oggetto di controllo e/o di verifica, estraendone eventualmente copia, nonché effettuare interviste e richiedere, se del caso, relazioni scritte. Nel corso di tali operazioni deve tenere costantemente informato il Responsabile dell'Ufficio o dell'unità organizzativa interessata.

L'**OdV**, a seguito delle verifiche effettuate, può segnalare al Responsabile gerarchico del soggetto che ha commesso la **Violazione** eventuali osservazioni e/o suggerimenti.

L'attività svolta dall'**OdV** deve essere documentata, anche in forma sintetica. La relativa documentazione deve essere custodita dallo stesso **OdV**, in modo che ne sia assicurata la riservatezza, anche nel rispetto della normativa in materia di protezione dei dati personali.

L'**OdV**, a seguito delle verifiche effettuate, delle modifiche normative di volta in volta intervenute nonché dell'eventuale insorgenza di nuovi processi a rischio, propone al Consiglio di Amministrazione gli adeguamenti e gli aggiornamenti del **Modello Organizzativo** che ritiene opportuni.

Per l'attività di verifica, l'**OdV** può avvalersi del supporto di Consulenti esterni con adeguate competenze in materia.

Ai fini specifici dell'esecuzione delle funzioni attribuite, il Consiglio di Amministrazione, tenuto conto anche delle attività dell'**OdV**, attribuisce allo stesso un *budget* per lo svolgimento dell'attività, al fine di assicurare adeguata autonomia economica e gestionale, fatto salvo il caso di urgenze documentate per le quali l'**OdV** può affrontare la spesa, informando il Presidente e dandone comunicazione al primo Consiglio di Amministrazione utile.

9.5 OBBLIGHI INFORMATIVI VERSO L'ORGANISMO DI VIGILANZA

Ai fini dell'efficace vigilanza sull'attuazione del **Modello Organizzativo**, i **Destinatari**, in ragione del proprio ruolo e delle proprie responsabilità, sono tenuti alla trasmissione dei flussi informativi verso l'**Organismo di Vigilanza** così come indicati nel **Modello Organizzativo**: le modalità e le tempistiche di flussi informativi *ad hoc* all'**OdV** per specifiche aree di attività a potenziale rischio-reato sono indicate in dettaglio nell'**Allegato 3** – *Flussi Informativi all'Organismo di Vigilanza*.

In ogni caso all'**OdV** sono conferiti tutti i poteri ai sensi del **Modello Organizzativo** per richiedere in ogni momento qualsiasi informazione, dato, documento, notizia ai **Destinatari**. I **Destinatari** dovranno fornire senza indugio quanto richiesto all'OdV.

Resta altresì fermo il principio che ogni informazione o notizia che ai sensi del **Modello Organizzativo** possa considerarsi rilevante dovrà essere trasmessa senza indugio all'**OdV**.

In aggiunta a quanto riportato in precedenza il **Vertice Aziendale** è tenuto a comunicare all'**Organismo**:

a. ogni cambiamento avente ad oggetto sia il sistema delle deleghe che la struttura organizzativa di **Qualitas Informatica**;
b. ogni nuova attività aziendale o apertura di sede;
c. ogni informazione rilevante per il rispetto, il funzionamento e l'aggiornamento del **Modello Organizzativo.**

L'eventuale omessa o ritardata comunicazione all'**OdV** dei flussi informativi sopra elencati sarà considerata violazione del **Modello Organizzativo** e potrà essere sanzionata secondo quanto previsto dal Sistema Disciplinare di cui al successivo paragrafo 11.

Le informazioni devono essere inoltrate con modalità telematica all'**OdV** all'indirizzo di posta elettronica odv231@qualitas.it ovvero anche in forma cartacea al seguente indirizzo: Qualitas Informatica S.p.A., alla c.a. dell'Organismo di Vigilanza, Via Vecchia Ferriera 5, 36100 - Vicenza (VI).

Le informazioni di cui sopra inviate all'**OdV** sono trattate e conservate dall'**OdV** medesimo in un apposito archivio informatico e/o cartaceo tenuto in conformità alle disposizioni di cui al Regolamento Europeo 2016/679 in tema di protezione dei dati personali (GDPR).

9.6 SEGNALAZIONI DI VIOLAZIONI-WHISTLEBLOWING

I **Destinatari** che decidono di effettuare una **Segnalazione** di **Violazione** devono attenersi alle modalità esposte nella *Policy Whistleblowing*.

In particolare, le Segnalazioni interne possono essere effettuate con le seguenti modalità:

indirizzo di posta cartacea *È necessario che la **Segnalazione interna** venga inserita in due buste chiuse: la prima con i dati identificativi del **Segnalante** unitamente alla fotocopia del documento di riconoscimento; la seconda con la **Segnalazione**. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura "Riservata al Gestore delle Segnalazioni"*	MN Tax & Legal – Corso di Porta Nuova, 46 – 20121 Milano
attraverso la piattaforma informatica raggiungibile al seguente link	https://whistleblowing-impresoftgroup.hawk-aml.com/Whistleblowing/home

Incontro diretto con il Gestore delle Segnalazioni	Incontro diretto da fissare via e-mail all'indirizzo whistleblowing@impresoft.com

Il divieto di ritorsione è previsto dall'art. 17 del D.Lgs. 24/2023, che si intende qui internamente richiamato[1]. Gli atti assunti in violazione di tale divieto sono nulli.

9.7 INFORMAZIONI DELL'ORGANISMO DI VIGILANZA AGLI ORGANI SOCIALI

L'**OdV** riferisce direttamente al Consiglio di Amministrazione in ordine alle tematiche inerenti al **Modello Organizzativo.**

L'**OdV informa**, anche per iscritto, **il Consiglio di Amministrazione** in merito all'applicazione e all'efficacia del Modello Organizzativo almeno semestralmente (indicando in particolare i controlli effettuati e l'esito degli stessi, nonché l'eventuale aggiornamento dei processi a rischio), o in tempi diversi con riferimento a specifiche ovvero significative situazioni.

L'**OdV potrà essere convocato dal Consiglio di Amministrazione** per riferire sulla propria attività e potrà chiedere di conferire con lo stesso. L'**OdV** potrà inoltre chiedere di essere sentito dal Consiglio di Amministrazione ogni qualvolta ritenga opportuno riferire tempestivamente in ordine a violazioni del **Modello Organizzativo** o richiedere l'attenzione su criticità relative al funzionamento ed al rispetto del **Modello Organizzativo** medesimo. In caso di necessità e/o urgenza l'**OdV** potrà conferire direttamente con il Presidente del Consiglio di Amministrazione.

L'**OdV** è competente a fornire i chiarimenti opportuni in presenza di problematiche interpretative o di quesiti relativi al **Modello Organizzativo**.

10. MODALITÀ DI GESTIONE DELLE RISORSE FINANZIARIE

L'articolo 6, comma 2 lettera c) del **Decreto Legislativo** richiede l'individuazione delle modalità di gestione delle risorse finanziarie idonee ad impedire la commissione dei reati.

Pertanto, **Qualitas Informatica** ha ritenuto opportuno, ad integrazione del **Modello Organizzativo**, emettere un Protocollo PT 2 "*Gestione dei Flussi Finanziari e Monetari*" e un Protocollo PT 3 *"Gestione contabile, predisposizione del bilancio d'esercizio ed*

[1] L'Art. 17 co. 1 "*Gli enti o le persone di cui all'articolo 3 non possono subire alcuna ritorsione*" si riferisce a:
a) i segnalanti (sì come definiti nella *Procedura Whistleblowing)*;
b) i facilitatori (sì come definiti nella *Procedura Whistleblowing)*;
c) le persone del medesimo contesto lavorativo (sì come definito nella *Procedura Whistleblowing*) del segnalante che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
d) i colleghi di lavoro del segnalante che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e attuale;
e) gli enti di proprietà del segnalante o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

adempimenti fiscali" che regolamentano, per ogni singola tipologia di transazione, i soggetti coinvolti ed i relativi poteri, gli strumenti adottati e i collegamenti con il sistema amministrativo/contabile.

SEZIONE III

11. SISTEMA DISCIPLINARE

11.1 PRINCIPI GENERALI

Il presente sistema disciplinare è adottato ai sensi dell'art. 6, comma secondo, lett. e) e dell'art. 7, comma quarto, lett. b) del **Decreto Legislativo.**

Il sistema è diretto a sanzionare le **Violazioni**, ivi incluse quelle accertate in seguito a **Segnalazione** (come descritto nella *Policy Whistleblowing*), in conformità alla normativa rilevante ed al CCNL di riferimento, laddove applicabile.

L'irrogazione di sanzioni disciplinari per **Violazione** dei Principi di Comportamento indicati nella Parte Speciale e nei Protocolli del **Modello Organizzativo** prescinde dall'eventuale instaurazione di un procedimento penale e dall'esito del conseguente giudizio per la commissione di uno dei reati previsti dal **Decreto Legislativo.**

11.2 AMBITO DI APPLICAZIONE

Il sistema disciplinare si applica a tutti i **Destinatari**, ed in particolare a:

- Dipendenti (Quadri e Impiegati);
- Dirigenti;
- Vertice Aziendale;
- Soggetti Terzi.

11.3 VIOLAZIONI

Le sanzioni potranno essere applicate nel caso di condotte consistenti:

a) in **Violazioni**;
b) nel mancato rispetto del **Codice Etico di Gruppo** e della *Policy Whistleblowing*;
c) in **Violazioni** integranti, direttamente o indirettamente, fattispecie di reato di cui al **Decreto Legislativo**;
d) nella mancata partecipazione, senza giustificato motivo, alla formazione erogata in materia di **Decreto Legislativo, Modello Organizzativo** e **Codice Etico di Gruppo**;
e) nella mancata o non veritiera evidenza dell'attività svolta relativamente alle modalità di documentazione, di conservazione e di controllo degli atti, in modo da impedire la trasparenza e verificabilità della stessa;
f) nel mancato rispetto e/o nell'elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione di supporto, ovvero nello svolgimento di attività volte ad impedire ai soggetti preposti e all'**OdV** il controllo o l'accesso alle informazioni richieste ed alla documentazione;
g) nell'inosservanza delle disposizioni relative ai poteri di firma e al sistema delle deleghe;
h) nel mancato rispetto degli obblighi di informazione nei confronti dell'**OdV**.

L'elenco delle fattispecie è a titolo esemplificativo e non tassativo.

11.4 CRITERI GENERALI DI IRROGAZIONE DELLE SANZIONI

Le eventuali inosservanze e/o violazioni del **Modello Organizzativo** vengono segnalate dall'**OdV**, oltre che al superiore gerarchico del soggetto interessato, anche al Presidente del Consiglio di Amministrazione competente per l'irrogazione delle sanzioni previste dalla legge.

Nei singoli casi di **Violazione**, il tipo e l'entità delle sanzioni specifiche verranno applicate in proporzione alla gravità delle mancanze e, comunque, in considerazione degli elementi di seguito elencati:

1. elemento soggettivo della condotta, a seconda del dolo o della colpa
2. rilevanza degli obblighi violati
3. livello di responsabilità gerarchica e/o tecnica
4. presenza di circostanze aggravanti o attenuanti con particolare riguardo alla professionalità, alle precedenti esperienze lavorative, alle circostanze in cui è stato commesso il fatto e ad eventuali recidive
5. eventuale condivisione di responsabilità con altri soggetti che abbiano concorso nel determinare la mancanza
6. comportamenti che possano compromettere, sia pure a livello potenziale, l'efficacia del **Modello Organizzativo**

Qualora con un solo atto siano state commesse più infrazioni, punite con sanzioni diverse, sarà applicata la sanzione più grave.

L'eventuale irrogazione della sanzione disciplinare, prescindendo dall'eventuale instaurazione del procedimento e/o dall'esito dell'eventuale giudizio penale, dovrà essere ispirata al principio di tempestività, per quanto possibile e compatibilmente con i CCNL applicabili. In ogni caso, la titolarità e l'esercizio del potere disciplinare o dell'esercizio dei diritti contrattuali deve essere esercitato nel rispetto del sistema di deleghe e procure in vigore.

11.5 SANZIONI PER I DIPENDENTI (QUADRI – IMPIEGATI)

Ai sensi del combinato disposto degli artt. 5, lettera b) e 7 del **Decreto Legislativo**, ferma la preventiva contestazione e la procedura prescritta dall'art. 7 della legge 20 maggio 1970 n. 300 (c.d. Statuto dei Lavoratori) nonché dal CCNL applicabile al personale dipendente di Qualitas Informatica, le sanzioni previste nel presente paragrafo potranno

essere applicate, tenuto conto dei criteri generali di cui sopra, nei confronti di quadri ed impiegati:

a) Richiamo verbale

La sanzione del rimprovero verbale potrà essere comminata nei casi di lieve inosservanza colposa dei Principi di Comportamento previsti dal Modello Organizzativo, del Codice Etico di Gruppo e/o della *Policy Whistleblowing* o di errori procedurali dovuti a negligenza non grave. Non necessita di preventiva contestazione.

b) Rimprovero scritto

Il provvedimento del rimprovero scritto si applica in caso di recidiva, da parte del lavoratore, nelle infrazioni che abbiano già dato origine ad ammonizione verbale di cui alla lettera a) o in caso di commissione di infrazioni.

c) Multa fino ad un massimo di 4 ore di retribuzione

Oltre che nei casi di recidiva nella commissione di inosservanze da cui possa derivare l'applicazione del rimprovero scritto, la multa (equivalente a massimo **quattro ore** di retribuzione) potrà essere applicata nei casi in cui, per il livello di responsabilità gerarchico o tecnico, il comportamento colposo e/o negligente sia di gravità tale da compromettere, sia pure a livello potenziale, l'efficacia del Modello Organizzativo.

d) Sospensione dalla retribuzione e dal servizio

La sanzione della sospensione dalla retribuzione e dal servizio (massimo **10 giorni**, graduati secondo la gravità dei fatti commessi) potrà essere comminata nei casi di inosservanza dei Principi di Comportamento e dei Protocolli del Codice Etico di Gruppo e/o della *Policy Whistleblowing*, tali da esporre Qualitas Informatica a responsabilità nei confronti dei terzi, nonché nei casi di recidiva nella commissione di inosservanze da cui possa derivare l'applicazione della multa. Inoltre, potrà essere comminata in caso di violazione delle misure a tutela del segnalante di cui al paragrafo 9.5 del Modello - Parte Generale - o di effettuazione con dolo o colpa grave di gravi segnalazioni che si rivelano, poi, del tutto infondate.

e) Licenziamento con preavviso

La sanzione del licenziamento con preavviso viene comminata in caso di plurima recidiva nelle mancanze previste nel punto precedente. Inoltre, potrà essere comminata nei casi in cui la violazione dei Principi di Comportamento e dei Protocolli, del Codice Etico di Gruppo e della *Policy Whistleblowing* sia avvenuta con dolo o colpa grave e riguardi aspetti nevralgici per Qualitas Informatica, al punto da non essere sufficiente la comminazione della sanzione della sospensione di cui al punto precedente.

f) Licenziamento senza preavviso

La sanzione del licenziamento senza preavviso con immediata risoluzione del rapporto di lavoro potrà essere comminata per mancanze così gravi da far venir meno il rapporto fiduciario con Qualitas Informatica e non consentire, pertanto, la prosecuzione neppure provvisoria del rapporto di lavoro, quali a titolo esemplificativo e non tassativo:

i. violazione dei Principi di Comportamento e dei Protocolli aventi rilevanza esterna e/o elusione fraudolenta degli stessi, realizzata con un comportamento diretto alla commissione di un illecito rilevante ai sensi del Decreto Legislativo, del Codice Etico di Gruppo e della *Policy Whistleblowing*;

ii. violazione e/o elusione del sistema di controllo, posta in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione ovvero mediante l'impedimento ai soggetti preposti e all'OdV del controllo o dell'accesso alle informazioni richieste ed alla documentazione.

Qualora il lavoratore sia incorso in una delle mancanze passibili di licenziamento senza preavviso Qualitas Informatica potrà disporre la sospensione cautelare del lavoratore con effetto immediato.

Nel caso in cui Qualitas Informatica decida di procedere al licenziamento, lo stesso avrà effetto dal giorno in cui ha avuto inizio la sospensione cautelare.

Ove i dipendenti sopra indicati siano muniti di procura con potere di rappresentare all'esterno Qualitas Informatica, l'irrogazione della sanzione può comportare la revoca della procura stessa.

11.6 SANZIONI PER I DIRIGENTI

Ai sensi del combinato disposto degli artt. 5, lettera b) e 7 del Decreto Legislativo e delle vigenti norme di legge e di contratto, le sanzioni indicate nel presente punto potranno essere applicate nei confronti dei dirigenti, osservando i criteri generali di irrogazione anche formali (contestazione scritta e richiesta di giustificazioni):

a) Richiamo scritto

La sanzione del richiamo scritto potrà essere irrogata nei casi di inosservanza colposa dei Principi di Comportamento e dei Protocolli di Controllo indicati nella Parte Speciale del Modello Organizzativo, del Codice Etico di Gruppo in caso di comportamenti illeciti individuati nella *Policy Whistleblowing*.

b) Licenziamento senza preavviso

La sanzione del licenziamento senza preavviso potrà essere irrogata nei casi da cui derivi una lesione del rapporto di fiducia tale da non consentire la prosecuzione, anche provvisoria, del rapporto di lavoro, quali a titolo esemplificativo e non tassativo:

i. violazione dei Principi di Comportamento e dei Protocolli aventi rilevanza esterna e/o l'elusione fraudolenta degli stessi realizzata con un comportamento diretto alla commissione di un illecito rilevante ai sensi del Decreto Legislativo, del Codice Etico di Gruppo e/o della *Policy Whistleblowing*;
ii. la violazione e/o l'elusione del sistema di controllo, poste in essere mediante la sottrazione, la distruzione o l'alterazione della documentazione ovvero nell'impedimento ai soggetti preposti e all'OdV del controllo o dell'accesso alle informazioni richieste ed alla documentazione.

Qualora il dirigente sia incorso in una delle mancanze passibili di licenziamento, Qualitas Informatica potrà disporne la sospensione cautelare con effetto immediato.

Nel caso in cui Qualitas Informatica decida di procedere al licenziamento, questo avrà effetto dal giorno in cui ha avuto inizio la sospensione cautelare.

Ove i dirigenti siano muniti di procura con potere di rappresentare all'esterno Qualitas Informatica, l'irrogazione della censura scritta potrà comportare anche la revoca della procura stessa.

11.7 SANZIONI PER IL VERTICE AZIENDALE

Le violazioni del **Modello Organizzativo** e/o del **Codice Etico di Gruppo** e/o della *Policy Whistleblowing* da parte del **Vertice Aziendale** vengono segnalate al Consiglio di Amministrazione che provvederà ad adottare i provvedimenti più idonei.

Tra le sanzioni applicabili al **Vertice Aziendale** vi sono: la revoca della delega, della procura e/o dell'incarico conferiti all'interessato e, qualora sia altresì legato alla Società da un rapporto di lavoro dipendente, potranno essere comminate le sanzioni di cui ai precedenti paragrafi 11.5 e 11.6.

Indipendentemente dall'applicazione della misura di tutela è fatta salva, comunque, la facoltà della **Società** di proporre azioni di responsabilità e/o risarcitorie.

11.8 VIOLAZIONI E SANZIONI PER I SOGGETTI TERZI

Qualitas Informatica ritiene che ogni comportamento posto in essere da Consulenti, Fornitori o altri soggetti aventi rapporti negoziali con Qualitas Informatica (anche "**Soggetti Terzi**") che possa comportare il rischio di commissione di uno dei **Reati** sia da censurare.

Pertanto, i Soggetti Terzi che abbiano:

a) violato i principi contenuti anche nel **Codice Etico di Gruppo** attinenti all'oggetto dell'incarico ovvero abbiano posto in essere un comportamento diretto alla commissione di un illecito rilevante ai sensi del **Decreto Legislativo** e/o che abbiano posto in essere i comportamenti illeciti individuati nella *Policy Whistleblowing*;

b) violato e/o eluso il sistema di controllo di **Qualitas Informatica**, anche attraverso la sottrazione, la distruzione o l'alterazione della documentazione attinente all'incarico ovvero abbiano impedito ai soggetti preposti e all'**OdV** il controllo e/o l'accesso alle informazioni richieste ed alla documentazione;

c) omesso di fornire a Qualitas Informatica e/o ai suoi organi di controllo la documentazione attestante l'attività svolta ovvero l'abbiano fornita incompleta o non veritiera impedendo così la trasparenza e verificabilità della stessa;

d) violato, anche attraverso comportamenti omissivi, norme, regolamenti e/o altre disposizioni aziendali in materia di tutela della salute e sicurezza sul lavoro, in relazione a tematiche ambientali;

verranno considerati quali inadempienti alle obbligazioni contrattuali assunte, con ogni conseguenza di legge; ciò può comportare - nei casi più gravi e coerentemente con le previsioni contrattuali - la risoluzione del contratto e/o la revoca dell'incarico nonché il risarcimento dei danni eventualmente subiti dalla **Società**.

SEZIONE IV

La presente Sezione IV del Modello Organizzativo rimanda ai documenti di **Parte Speciale** ed ai **Protocolli**, i cui principi di comportamento e meccanismi di controllo devono essere osservati dai Destinatari al fine di eliminare o, almeno, ridurre ad un livello accettabile il rischio di comportamenti integranti uno dei reati la cui commissione può comportare l'applicazione delle sanzioni previste dal Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche ed integrazioni.

12. PROTOCOLLI

- **PT1 – Gestione dei rapporti con la Pubblica Amministrazione;**
- **PT2 – Gestione dei flussi finanziari e monetari;**
- **PT3 – Contabilità, bilancio ed adempimenti fiscali;**
- **PT4 – Gestione degli acquisti di beni, servizi e consulenze;**
- **PT5 – Gestione delle attività commerciali, dello sviluppo software e del marketing;**
- **PT6 – Gestione della salute e sicurezza nei luoghi di lavoro e della tutela ambientale;**
- **PT7 – Selezione, assunzione e gestione del personale;**
- **PT8 – Gestione dei rapporti Intercompany;**
- **PT9 – Gestione del sistema informativo.**

Qualitas Informatica S.p.A
Società a Socio Unico
Sede legale ed Amm.va:
Via Vecchia Ferriera 5 - 36100 Vicenza
Società soggetta all'attività di Direzione e Coordinamento di Impresoft S.p.A

Qualitas
AN IMPRESOFT COMPANY

Vicenza (VI), lì 4 Agosto 2025

OGGETTO: ADOZIONE MODELLO ORGANIZZATIVO EX D.LGS. 231/2001 E NOMINA ORGANISMO DI VIGILANZA

Il Legale Rappresentante rende noto ai responsabili di ciascuna Area, ai dipendenti, collaboratori, fornitori, *outsourcer*, partner, consulenti esterni e a coloro che pur non appartenendo alla società Qualitas Informatica S.p.A. (la "**Società**") operano su mandato o per conto della stessa che, con l'approvazione del modello di organizzazione gestione e controllo (il "**Modello**") da parte del Consiglio di Amministrazione in data 21 Gennaio 2025 si è concluso il percorso attuativo della disciplina prevista dal D.lgs. 231 del 2001 (il "**Decreto**"). Tale lavoro è coinciso con le attività necessarie che la Società ha posto in essere per adeguare la propria organizzazione e il proprio funzionamento alla disciplina introdotta nell'ordinamento giuridico italiano dalla succitata norma.
Come è noto, tale Decreto disciplina la responsabilità degli enti per determinati reati commessi nell'interesse o a vantaggio degli stessi da coloro che rivestono, anche di fatto, funzioni di rappresentanza, amministrazione o direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati.
Gli enti possono andare esenti da questa responsabilità (che prevede sanzioni economiche e sanzioni interdittive) **adottando ed attuando efficacemente un Modello** così come previsto dall'art. 6 del D.Lgs. 231/01.
Inoltre, si segnala che, secondo le previsioni dell'art. 6 del Decreto, il Consiglio di Amministrazione ha istituito l'Organismo di Vigilanza (anche solo "**OdV**") in forma monocratica nella persona dell'Avv. Giacomo Escobar.
Le comunicazioni all'OdV possono essere recapitate con le seguenti modalità:
- a mezzo e-mail all'indirizzo: odv231@qualitas.it
- a mezzo posta all'indirizzo della Società: Att.ne Organismo di Vigilanza, Via Vecchia Ferriera, 5, 36100, Vicenza (VI).

Con i migliori saluti.

Il Legale Rappresentante
Sergio Gasparin

QUALITAS INFORMATICA SpA
Via Vecchia Ferriera, 5
36100 VICENZA
P.I./C.F.: 01833260241
Tel. 0445.641844

Livello di classificazione del documento	Pubblico		Interno		Riservato		Segreto	