# Modello Organizzativo

## Estratto parte generale-speciale-sist.sanzionatorio

## Ex D.Lgs 231/01

Sommario

# 1 SEZIONE INTRODUTTIVA

## 1.1 Premessa

Il presente documento è stato sviluppato in conformità a quanto prescritto dalla linea guida CONFINDUSTRIA, nel **"CODICE DI COMPORTAMENTO E LINEE GUIDA PER LA PREDISPOSIZIONE DEI MODELLI ORGANIZZATIVI E GESTIONALI AI SENSI DEL DECRETO LEGISLATIVO N. 231/2001"**, approvato dal Ministero della Giustizia il 17 aprile 2013 e aggiornato a Giugno 2021.

Il D.Lgs. 231/2001, recante la "Disciplina della responsabilità amministrativa delle persone giuridiche, delle Azienda e delle associazioni anche prive di personalità giuridica" ha introdotto per la prima volta in Italia la responsabilità in sede penale degli enti per alcuni reati commessi nell'interesse o a vantaggio degli stessi, da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale, nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso (cosiddetti soggetti apicali) e, infine, da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti sopra indicati (cosiddetti soggetti sottoposti ad altrui direzione).

La responsabilità introdotta dal D.Lgs. 231/2001 mira a coinvolgere nella punizione di taluni illeciti penali il patrimonio degli enti che abbiano tratto un vantaggio dalla commissione dell'illecito. Per tutti gli illeciti commessi è sempre prevista l'applicazione di una sanzione pecuniaria; per i casi più gravi sono previste anche misure interdittive quali la sospensione o revoca di licenze e concessioni, il divieto di contrarre con la Pubblica Amministrazione, l'interdizione dall'esercizio dell'attività, l'esclusione o revoca di finanziamenti e contributi, il divieto di pubblicizzare beni e servizi.

L'obiettivo che SERENITY intende perseguire adottando il Modello Organizzativo è plurimo:

- favorire un approccio costruttivo verso tutti gli interlocutori
- prevenire comportamenti illeciti nella gestione dei processi ed attività svolte dall'organizzazione
- rendere consapevoli tutte le persone facenti parte della struttura dell'organizzazione, sia di governo sia esecutiva, che eventuali comportamenti illeciti possono comportare sanzioni penali ed amministrative sia per il singolo che per l'azienda

Il presente documento è stato allineato anche ai requisiti della norma internazionale ISO 37001: 2016 "Sistema di gestione per la prevenzione della corruzione. Requisiti" per tener conto delle misure organizzative e tecniche che l'azienda adotta al fine di prevenire qualsivoglia evento di natura corruttiva.

## 1.2 Presentazione della SERENITY S.p.A.

Serenity è da oltre 30 anni leader italiano degli ausili assorbenti per l'incontinenza.

Serenity propone una gamma completa di prodotti adatta per ogni tipologia di incontinenza, da leggera a severa, per il benessere dei propri assistiti, con l'obiettivo di restituire loro un sereno ottimismo, basato sull'ascolto, sulla professionalità e su risposte semplici, concrete e innovative.

Lo stabilimento sorge in zona industriale su un'area di 160.000 $m^2$ di cui 38.000 $m^2$ per fabbricato.

Il CSS (Centro Studi Serenity) e i laboratori di Ricerca e Sviluppo interni alla propria unità produttiva (situata in Ortona - Chieti) concorrono costantemente al raggiungimento del massimo livello qualitativo del prodotto, attraverso il continuo aggiornamento tecnologico, il superamento di test clinici e di laboratorio, la raccolta di informazioni e stimoli dal mercato e la cooperazione con gruppi multi-disciplinari di specialisti medici (geriatri, urologi, andrologi e psicologi).

La collaborazione con Istituti e Università è essenziale per lo sviluppo di temi specifici e innovativi: Serenity affida la consulenza medico-scientifica e la formazione degli operatori in ambito geriatrico, sanitario e assistenziale a GRG (Gruppo di Ricerca Geriatrica di Brescia) e approfondisce le conoscenze professionali e scientifiche relative al mondo dell'incontinenza attraverso la cooperazione con FINCO (Federazione Italiana Incontinenti) e AILSLeC (Associazione Infermieristica per lo Studio delle Lesioni Cutanee).

La Società aderisce ai valori del gruppo ONTEX, valori che oltre ad essere ben definiti nei documenti direzionali aziendali sono resi pubblici, anche in lingua italiana, sul sito del gruppo (www.ontexglobal.com), dove sono reperibili i documenti che indicano la nostra visione, i nostri valori, il nostro codice etico, il nostro business model e il nostro impegno per una crescita ed una produzione sostenibili.

Per tutti i riferimenti societari in termini di attività svolte, composizione sociale, poteri degli organi direzionali e amministrativi, si rimanda allo Statuto di Serenity.

### 1.3 Riferimenti normativi generali

| CODICE | *Titolo/ Ambito* |
|---|---|
| D.Lgs 231/01 | *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle Azienda e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300"* |
| --- | Statuto aziendale |
| Legge 23 novembre 2001, n. 409 | *Introduzione dei reati di fede pubblica* |
| D. lgs. 11 aprile 2002, n. 61 | *Introduzione dei reati societari* |
| Legge 14 gennaio 2003 n. 7 | *Introduzione dei reati di terrorismo* |
| Legge 11 agosto 2003 n. 228 | *Introduzione dei delitti contro la persona e la personalità individuale* |
| Legge 18 aprile 2005, n. 62 | *Introduzione dei reati e illeciti amministrativi e abusi di mercato* |
| Legge 9 gennaio 2006, n. 7 | *Introduzione dei reati legati alle pratiche di mutilazione degli organi genitali femminili* |
| Legge 16 marzo 2006, n. 146 | *Introduzione dei reati transnazionali* |
| Legge 3 agosto 2007, n. 123 | *Introduzione dei reati di omicidio colposo e lesioni colpose gravi o gravissime, commesse con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della sicurezza sul lavoro* |
| D.lgs. 21.11.2007, n. 231 | *Introduzione dei reati di ricettazione e riciclaggio* |
| Legge 18 marzo 2008, n. 48 | *Introduzione dei reati informatici* |
| Legge 15 luglio 2009 n. 94 | *Introduzione dei delitti di criminalità organizzata* |
| Legge 23 luglio 2009, n. 99 | *Introduzione dei reati di violazione del diritto d'autore e reati contro l'industria e il commercio* |
| Legge 3 agosto 2009, n. 116 | *Introduzione dei reati relativi all'induzione a non rendere dichiarazioni o rendere dichiarazioni mendaci all'autorità giudiziaria* |
| D.Lgs 121/2011 | *Introduzione dei reati ambientali* |

| CODICE | *Titolo/ Ambito* |
|---|---|
| D.Lgs 109/2012 | *Introduzione dei reati di immigrazione clandestina e lavoratori irregolari* |
| LEGGE 6 novembre 2012, n. 190 | *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione* |
| LEGGE 15 dicembre 2014, n. 186 | *Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di Autoriciclaggio* |
| LEGGE 22 maggio 2015, n. 68 | *Disposizioni in materia di delitti contro l'ambiente* |
| LEGGE 27 maggio 2015, n. 69 | *Disposizioni in materia di delitti contro la pubblica amministrazione, di associazioni di tipo mafioso e di falso in bilancio* |
| D.Lgs. 81/2008 e s.m.i. | *Testo Unico Sicurezza sul lavoro* |
| D.Lgs. 152/2006 e s.m.i. | *Testo Unico Ambientale* |
| Legge n°300/1970 | *Statuto dei Lavoratori* |
| Legge 190/2012 | *Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione* |
| PNA | *Piano Nazionale Anticorruzione (P.N.A.) e relativi allegati* |
| Determina ANAC n.831 del 3 agosto 2016 | *Determinazione di approvazione definitiva del Piano Nazionale Anticorruzione 2016* |
| Reg. EU 679/2016 | *Regolamento per la protezione dei dati personali* |
| D.Lgs 90/2017 | *Attuazione della direttiva (UE) 2015/849 relativa alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo ….* |
| Legge 167/2017 | *Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea – Legge Europea 2017 (istigazione ed incitamento al razzismo ed alla xenofobia)* |
| Legge 179/2017 | *Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato (whistleblowing)* |
| D.Lgs. 101/2018 | Adeguamento al Regolamento UE 679/ 2016 |
| ISO 31000: 2018 | Principi e Linee Guida per la Gestione del Rischio. Versione italiana dello standard internazionale di riferimento per la gestione del rischio. Definisce i principi generali, la struttura organizzativa di riferimento e gli elementi del processo per la gestione dei rischi |
| ISO 37001: 2016 | Sistema di gestione per la prevenzione della corruzione. Requisiti |
| LEGGE 9 gennaio 2019, n. 3 | Misure per il contrasto dei reati contro la pubblica amministrazione, nonchè in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici |
| D.L. 26 ottobre 2019, n. 124 | Inserimento dell'art. 25 quinquiesdecies al D.Lgs. 231/2001 (previsti cioè nel novellato D.Lgs. 74/2000) |
| Direttiva 1937/2019 | Direttiva riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (whistleblowing) |

| CODICE | *Titolo/ Ambito* |
|---|---|
| Direttiva (UE) 2017/1371 del 5 luglio 2017 | Direttiva relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale |
| D. Lgs. 75/2020 | Attuazione della Direttiva UE 1371/2017 (Direttiva PIF), relativa alla lotta contro le frodi che ledono gli interessi finanziari dell'Unione mediante il diritto penale (reati di contrabbando) |
| D.L. 4/2021 | Ratifica ed esecuzione della Convenzione dell'Organizzazione internazionale del lavoro n. 190 sull'eliminazione della violenza e delle molestie sul luogo di lavoro, adottata a Ginevra il 21 giugno 2019 nel corso della 108ª sessione della Conferenza generale della medesima Organizzazione |
| D.Lgs 184/2021 | Attuazione della direttiva (UE) 2019/713 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti e che sostituisce la decisione quadro 2001/413/GAI del Consiglio. |
| Delibera ANAC numero 469 del 09/06/2021 | Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro |
| Linea Guida Confindustria Giugno 2021 | Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo |
| D.Lgs 195/2021 | Attuazione della direttiva (UE) 2018/1673 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla lotta al riciclaggio mediante diritto penale |
| ISO 37301: 2021 | Compliance management systems – Requirements with guidance for use |
| ISO 37000: 2021 | Governance delle organizzazioni. Linea guida |
| ISO 37002: 2021 | Whistleblowing management systems — Guidelines |
| Legge 9 marzo 2022, n. 22 | Disposizioni in materia di reati contro il patrimonio culturale<br>(approvata dalla Camera il 18 ottobre 2018 e dal Senato con modifiche il 14 dicembre 2021) |
| Strategia UE Gender Equality | Strategia europea per la parità di genere 2020-2025 |
| Decreto del 7 maggio 2022 | Determinazione del costo medio dei rimpatrio per l'anno 2022 a carico dei datori di lavoro che impiegano cittadini di paesi terzi il cui soggiorni è irregolare. (Art. 22, comma 12-ter. D.Lgs. 286/98) |
| D.Lgs. n.156 del 4.10.22 | Disposizioni correttive e integrative del decreto legislativo 14 luglio 2020, n. 75, di attuazione della direttiva (UE) 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale |
| D.Lgs. n.150 del 10.10.22 | "Attuazione della legge 27 settembre 2021, n. 134, recante delega al Governo per l'efficienza del processo penale, nonché in materia di giustizia riparativa e disposizioni per la celere definizione dei procedimenti giudiziari" |
| Piano ANAC del 05/12/2022 | Piano Nazionale Anticorruzione (PNA) 2022<br>(approvato dal Consiglio dell'Anac il 16 novembre 2022) |

## 1.4 Definizioni

Al presente documento si applicano le seguenti definizioni:

| | |
|---|---|
| D.Lgs. 231/01 | il Decreto Legislativo dell'8 giugno 2001 n. 231, recante «Disciplina della responsabilità amministrativa delle persone giuridiche, delle Azienda e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300», e successive modifiche ed integrazioni |
| Collaboratori | Sono i soggetti che intrattengono con SERENITY rapporti di collaborazione coordinata e continuativa prevalentemente personale e senza vincolo di subordinazione (quali, a titolo esemplificativo e non esaustivo, lavoro a progetto, lavoro somministrato) ovvero qualsiasi altro rapporto contemplato dall'art. 409 del codice di procedura civile, le prestazioni di lavoro occasionale, nonché qualsiasi altra persona sottoposta alla direzione o vigilanza di qualsiasi soggetto in posizione apicale di SERENITY ai sensi del decreto legislativo 8 giugno 2001, n. 231 |
| Destinatari | Sono i soggetti a cui si applicano le disposizioni del presente Modello Organizzativo e, in particolare, i Dipendenti, i Responsabili, i Collaboratori a vario titolo e gli Esponenti Aziendali |
| Dipendenti | Sono i soggetti che intrattengono con SERENITY un rapporto di lavoro subordinato, inclusi i lavoratori a termine o a tempo parziale |
| "Ente" o "Organizzazione" | Con tali termini si indica un insieme di persone e di mezzi, con definite responsabilità, autorità ed interrelazioni (Fonte UNI EN ISO 9000: 2005) - Esempio: Azienda, raggruppamento di Azienda, azienda, impresa, istituzione, organismo umanitario, concessionario, associazione, o loro parti o combinazioni. Il legislatore, nel redigere il D.Lgs.231/2001, ha usato i termini nella stessa accezione |
| Esponenti Aziendali"<br>(soggetti apicali) | Sono, come di volta in volta in carica, il Amministratore Delegato e i membri del CdA, nonché qualsiasi altro soggetto in posizione apicale, per tale intendendosi qualsiasi persona che rivesta funzioni di rappresentanza, amministrazione o direzione di SERENITY o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale ai sensi del decreto legislativo 8 giugno 2001, n. 231 |
| Organismo di Vigilanza | È l'Organismo di Vigilanza (abbreviato OdV) dotato di autonomi poteri di iniziativa e controllo, in conformità al decreto legislativo 8 giugno 2001, n. 231 |
| Stakeholders | Il termine, coniato nel 1963 dal Research Institute dell'Azienda di Stanford ed ormai entrato nel dizionario comune delle strategie d'impresa, individua tutti i soggetti "portatori di interessi" nei confronti di una iniziativa economica, sia essa un'azienda sia esso un progetto; fanno parte di questo insieme gli utenti, i fornitori, i soci, i collaboratori ma anche gruppi di interesse esterni come i cittadini residenti che vivono sul territorio o gruppi di interesse locale. |
| Protocolli | Il termine individua una tipologia di attività ritenuta idonea a prevenire i reati di cui al D.Lgs.231/01. Con il termine, nel presente documento, sono anche indicati tutti i documenti prescrittivi del Modello (Documentazione varia, come da Elenco Generale dei Documenti), che evidenziano le procedure ed i controlli preventivi attuati dall'azienda |
| Delega | L'ordine delle competenze può essere derogato con la delega, l'atto attraverso la quale un organo (delegante) trasferisce ad un altro organo (delegato) l'esercizio di poteri e facoltà rientranti nella sua sfera di competenza. Poiché deroga l'ordine delle competenze, il potere di delega deve essere conferito da una norma avente forza non inferiore a quella che ha attribuito le competenze derogate.<br><br>La delega si distingue dalla rappresentanza perché quest'ultima da luogo ad un rapporto giuridico intercorrente tra distinti soggetti giuridici (il rappresentante e il rappresentato), laddove la delega intercorre tra due organi (il delegante e il delegato) dello stesso soggetto.<br><br>La delega si distingue inoltre dalla supplenza, che si ha quando un organo (supplente) esercita le competenze spettanti ad altro organo, a seguito dell'impossibilità di quest'ultimo di funzionare, per assenza o impedimento del suo titolare. Anche la supplenza deve essere prevista da una norma avente forza non inferiore a quella che ha conferito la competenza. Di solito le norme che prevedono la supplenza prestabiliscono in via generale l'organo (detto vicario) destinato a funzionare quale supplente di un altro |

| | |
|---|---|
| Conflitto di competenza | Si ha un conflitto di competenza quando due o più organi contemporaneamente affermano (conflitto positivo) o negano (conflitto negativo) la propria competenza riguardo ad una determinata questione (conflitto reale) oppure vi è la possibilità che tale contrasto abbia luogo (conflitto virtuale). |
| Procura | La procura è un atto unilaterale con il quale un soggetto investe un altro soggetto del potere di rappresentarlo; ed è un atto unilaterale non eccettizio; è rivolto cioè, non ad un destinatario determinato, ma alla generalità dei terzi, di fronte ai quali il rappresentato legittima il rappresentate a contrattare in suo nome |
| Autoriclaggio | Reato per cui, chiunque, avendo commesso o concorso a commettere un delitto non colposo, impiega, sostituisce, trasferisce, in attività economiche, finanziarie, imprenditoriali o speculative, il denaro, i beni o altre utilità provenienti dalla commissione di tale delitto, in modo da ostacolare concretamente l'identificazione della loro provenienza delittuosa |
| Informazioni privilegiate | ▪ Il concetto di informazione privilegiata rappresenta il fulcro attorno al quale ruota l'intera disciplina sull'insider trading e quella concernente l'informazione societaria disciplinata nel Titolo III, Capo I, art. 114 e seguenti del TUF e nel Regolamento di attuazione del TUF concernente la disciplina degli emittenti adottato dalla Consob con delibera n. 11971 del 14 maggio 1999 e successive modifiche e integrazioni (qui di seguito il "Regolamento Emittenti").<br>Secondo quanto previsto dall'art. 181 del TUF si ritengono di carattere privilegiato le informazioni aventi le seguenti caratteristiche (qui di seguito le "Informazioni Privilegiate"):<br>o di carattere preciso, nel senso che:<br>i) deve trattarsi di informazioni inerenti a circostanze o eventi esistenti o verificatisi o a circostanze o eventi che ragionevolmente possa prevedersi che verranno ad esistenza o che si verificheranno (il riferimento è ai casi in cui la notizia è in via di formazione e riguarda eventi non ancora verificatisi, si pensi al caso caratterizzato dalla notizia che una società quotata stia per lanciare un'OPA, oppure il caso riguardante un piano strategico di riposizionamento produttivo di una società emittente titoli quotati nei mercati regolamentati italiani)<br>ii) deve trattarsi di informazioni specifiche, vale a dire che l'informazione deve essere sufficientemente esplicita e dettagliata, in modo che chi la impiega sia posto in condizione di ritenere che dall'uso potranno effettivamente verificarsi quegli effetti sul prezzo degli strumenti finanziari<br>o non ancora rese pubbliche<br>o concernenti, direttamente o indirettamente, uno o più emittenti strumenti finanziari quotati nei mercati regolamentati italiani o uno o più strumenti finanziari negoziati sul mercato dei capitali (il riferimento riguarda sia le cd. corporate information, cioè le informazioni relative a fatti generati o provenienti dalla società emittente relativi, ad esempio, alla situazione economica patrimoniale o a vicende organizzative dell'emittente, sia le cd. market information, cioè le informazioni relative a fatti generati al di fuori della sfera dell'emittente e che abbiano un significativo riflesso sulla market position dell'emittente)<br>o "price sensitive" secondo l'investitore ragionevole, nel senso che deve trattarsi di un'informazione che, se resa pubblica, presumibilmente un investitore ragionevole utilizzerebbe come uno degli elementi su cui fondare le proprie decisioni di investimento. |
| Corruzione | ▪ Offrire, promettere, fornire, accettare o richiedere un **vantaggio indebito di qualsivoglia valore** (che può essere economico o non economico), direttamente o indirettamente, e indipendentemente dal luogo, violando Ia legge vigente, come incentivo o ricompensa per una persona ad agire o a omettere azioni in relazione alla *prestazione* delle mansioni di quella persona |
| Whistleblowing | ▪ Segnalazione di denuncia di attività illecite o fraudolente all'interno di una organizzazione operata da parte di un segnalatore connesso all'organizzazione stessa |
| Violenze e molestie | ▪ insieme di pratiche e di comportamenti inaccettabili, o la minaccia di porli in essere, sia in un'unica occasione, sia ripetutamente, che si prefiggano, causino o possano comportare un danno fisico, psicologico, sessuale o economico; l'espressione include la violenza e le molestie di genere |
| violenza e molestie di genere | ▪ la violenza e le molestie nei confronti di persone in ragione del loro sesso o genere, o che colpiscano in modo sproporzionato persone di un sesso o genere specifico, ivi comprese le molestie sessuali. |

## 1.5 Abbreviazioni

| | | | |
|---|---|---|---|
| **CdA** | Consiglio di Amministrazione | **AD** | Amministratore Delegato |
| **ODV** | Organismo di Vigilanza | **D.Lgs** | Decreto Legislativo |
| **OMI** | Ontex Manufacturing Italia | **PA** | Pubblica Amministrazione |
| **FDC** | Funzione di Conformità | | |

# 2 INTRODUZIONE AL MODELLO ORGANIZZATIVO 231

## 2.1 Considerazioni generali

Il D.Lgs. n.231/2001 (nel seguito indicato anche come "Decreto"), adottato in adempimento di strumenti comunitari e internazionali (Convenzione PIF e OCSE), ha introdotto nel nostro ordinamento una forma di responsabilità sanzionatoria da reato degli enti collettivi (provvisti o meno di responsabilità giuridica, fatta eccezione per lo Stato, gli altri Enti territoriali e gli enti pubblici che esercitano una pubblica funzione).

Detta responsabilità sanzionatoria è qualificata come "amministrativa", anche se non manca chi vi riconosce i segni di un'autentica responsabilità penale, in considerazione della natura afflittiva delle sanzioni, dei loro scopi (di prevenzione generale e speciale), del piano dei beni tutelati e del procedimento applicativo, interamente devoluto al giudice penale. Il nucleo essenziale della riforma può essere compendiato nel modo seguente: la Azienda *può* essere sottoposta a sanzioni (vedremo fra breve quali) quando un determinato reato (previsto nella "parte speciale" del decreto) viene commesso, ***nel suo interesse o a suo vantaggio***, da un soggetto che, nell'organigramma societario, riveste una posizione ***apicale*** (amministratore, Amministratore Delegato, rappresentante, Amministratore Delegato) ovvero la qualità di ***dipendente***.

Quello ora delineato costituisce il requisito di ***imputazione oggettiva*** del reato all'ente (v. art. 5 del Decreto), cioè il criterio di ascrizione normativa del fatto-reato alla persona giuridica nell'interesse o a vantaggio della quale la persona fisica ha agito (cd. "teoria dell'identificazione o dell'immedesimazione organica"). Tuttavia, la responsabilità sanzionatoria dell'ente si perfeziona solo se ricorrono anche i requisiti dell'***imputazione soggettiva*** stabiliti negli artt. 6 e 7 del Decreto.

Il modello di prevenzione-minimizzazione del rischio-reato ha attivato, dal proprio interno, tutti i meccanismi di ***identificazione, gestione e controllo del rischio,*** tenendo conto della tipologia dell'attività, della storia ed ubicazione dell'ente, delle caratteristiche dei suoi *stakeholders*, delle possibili modalità di attuazione degli illeciti.

La SERENITY S.p.A., nell'ottica della gestione dinamica della fase di *risk assessment*, ha predisposto una matrice di correlazione rischio reato/processi aziendali che definisce puntualmente le aree di rischio. Nella matrice sono anche individuati i nominativi dei Process Owner (riconducibili ai singoli processi aziendali).

## 2.2 La struttura del modello di organizzazione

Il Modello di Organizzazione, Gestione e Controllo ex D.Lgs.231/01, adottato da SERENITY, è sviluppato secondo due livelli di presentazione:

- una parte tesa a individuare la fisionomia istituzionale del Modello (parte generale)
- una parte indirizzata a setacciare e regolare le attività esposte al rischio-reato (parte speciale).

La struttura del modello include i riferimenti alle procedure e protocolli che si ritengono a rischio per una specifica macrofamiglia di reati, sulla base del *risk assessment*, così da individuare in modo puntuale e preciso:

1. i reati presupposto ritenuti critici
2. le aree di rischio nelle quali possono presentarsi eventi anomali collegati ai reati di cui in precedenza
3. le procedure aziendali afferenti le aree a rischio
4. i Process Owner dei processi a rischio reato.

Costituiscono inoltre parte integrante del Modello adottato da SERENITY:

- Statuto, che costituisce il documento fondamentale su cui è basato il sistema di governo dell'organizzazione: definisce lo scopo, la sede, l'oggetto sociale, il capitale sociale, nonché i compiti e le responsabilità dei Soggetti apicali
- Business Model, che rappresenta il riferimento primario per la definizione delle modalità organizzate attraverso le quali l'azienda gestisce le proprie attività di business
- Codice Etico, approvato dal CdA, che fissa le linee di comportamento generali e rappresenta l'insieme dei valori nei quali SERENITY si riconosce e che la caratterizzano, ai quali si attiene nell'espletamento della propria attività e la cui osservanza è imprescindibile per l'affidabilità, la reputazione e l'immagine di SERENITY e che i soci, gli amministratori, i dipendenti e i collaboratori si impegnano ad osservare ed, in via indiretta, a far osservare ai fornitori ed ai soggetti terzi che hanno rapporti contrattuali con la SERENITY. Tale documento viene predisposto, adottato e diffuso da SERENITY seguendo le regole descritte nel presente documento
- Regolamento dell'Organismo di Vigilanza. Tale regolamento è adottato direttamente dall'Organismo di Vigilanza in virtù dei principi di autonomia ed indipendenza. Al CdA spetta di deliberare circa l'istituzione di un Organismo deputato a vigilare sull'efficacia, sul corretto funzionamento e sull'osservanza del Modello, nonché di curarne l'aggiornamento e valutarne la coerenza con gli obiettivi prefissati da SERENITY relativamente all'istituzione del Modello. Tale Organismo, la cui composizione deve rispettare alcuni requisiti individuati direttamente dal CdA, è dotato di autonomi poteri di iniziativa e di controllo
- Organigramma, Job Description e relativa articolazione dei Poteri e Sistema delle Deleghe che regolamentano la struttura organizzativa, l'articolazione dei poteri e descrivono il sistema delle deleghe vigente in SERENITY. Tale definizione della struttura organizzativa mira a garantire una chiara ed organica attribuzione dei compiti (prevedendo per quanto possibile una chiara segregazione delle funzioni o in alternativa, controlli compensativi), coerente con le responsabilità assegnate e che assicuri una chiara e trasparente rappresentazione del processo aziendale di formazione e di attuazione delle decisioni ed a controllare la correttezza dei comportamenti.
- Sistema Disciplinare e Sanzionatorio compatibile con i vigenti Contratti Collettivi Nazionali (CCNL) nonché con gli accordi integrativi presenti, che sanzioni comportamenti in contrasto o che violano le regole di condotta definite dall'azienda ed imposte dal Modello ai fini della prevenzione dei reati di cui al Decreto. L'applicazione delle sanzioni disciplinari prescinde dall'esito di un eventuale procedimento penale, in quanto le regole di condotta imposte dal Modello sono assunte dall'azienda in piena autonomia indipendentemente dall'illecito che eventuali condotte possano determinare.
- Protocolli (manuali ed informatici) formalizzati tese a disciplinare le modalità operative per assumere ed attuare decisioni nei settori "sensibili", individuabili all'interno delle parti speciali del modello perché poste in evidenza nella mappatura dei processi aziendali, con particolare attenzione all'area amministrativa/contabile.
- Piano di Formazione che preveda, specie per il personale apicale impegnato in aree sensibili, formazione in materia di prevenzione nella realizzazione di illeciti e comunque di tutto ciò che è oggetto del Decreto e del Modello adottato dall'azienda; un piano di informazione di tutti i soggetti interessati (fornitori, consulenti, partner, etc.); in sintesi, dal piano emergono le linee dell'attività di informazione e di formazione sui contenuti del Modello e dei protocolli di gestione del rischio-reato

In considerazione di quanto sopra, l'Organismo di Vigilanza ha il compito di adottare ogni tipo di provvedimento affinché il CdA provveda ad operare tutti gli aggiornamenti ed integrazioni necessari per il Modello.

## 2.3 Comunicazione, diffusione, attuazione e aggiornamento del Modello

### *2.3.1 Comunicazione e diffusione del Modello*

Ai fini dell'efficacia del presente Modello, è obiettivo di SERENITY garantire una corretta conoscenza e divulgazione delle regole di condotta ivi contenute. Il livello di formazione ed informazione è attuato con un diverso grado di approfondimento in relazione al diverso livello di coinvolgimento delle risorse nelle attività sensibili, nonché della qualifica dei destinatari.

L'adozione del Modello è comunicata al momento dell'adozione stessa sia al personale dell'azienda, sia ai fornitori e consulenti della medesima. Ai nuovi assunti/ collaboratori/ ricercatori e a chiunque entrasse a far parte dell'organizzazione di SERENITY, viene consegnato un set informativo, con il quale assicurare agli stessi le conoscenze considerate di primaria importanza, relativamente al Modello.

Tali soggetti saranno tenuti a rilasciare a SERENITY una dichiarazione sottoscritta ove si attesti la ricezione di tale set informativo, nonché la integrale conoscenza dei documenti allegati e l'impegno ad osservarne le prescrizioni.

Il sistema di formazione, informazione e comunicazione è soggetto alla supervisione, nonché è integrato dall'attività realizzata in questo ambito dall'Organismo di Vigilanza.

I consulenti e collaboratori, e comunque le persone fisiche o giuridiche con cui SERENITY addivenga ad una qualsiasi forma di collaborazione contrattualmente regolata, ove destinati a cooperare con l'azienda nell'ambito delle attività in cui ricorre il rischio di commissione dei reati, devono essere informati del contenuto del Modello e dell'esigenza dell'azienda che il loro comportamento sia conforme al Modello e ai principi etico-comportamentali adottati da SERENITY.

### *2.3.2 Attuazione del Modello*

La decisione circa la necessità di procedere all'attuazione del Modello spetta al CdA, dotandosi, direttamente o indirettamente, delle risorse necessarie, che istituisce un OdV, con il compito specifico di

- ratificare/ validare la struttura del sistema dei flussi informativi e dei relativi supporti informatici e, in base ai contenuti del Modello, verificarne l'attuazione
- monitorare l'applicazione del Modello nelle sedi pertinenti, istituendo gli opportuni canali di comunicazione.

### *2.3.3 Aggiornamento del Modello*

In tutte le occasioni in cui sia necessario procedere a interventi di aggiornamento e adeguamento del Modello deve essere predisposto un programma che individui le attività necessarie con definizione di responsabilità, tempi e modalità di esecuzione.

Tale aggiornamento si rende in particolare necessario in occasione:

- dell'introduzione di novità legislative
- di casi significativi di violazione del Modello e/o esiti di verifiche sull'efficacia del medesimo o esperienze di pubblico dominio del settore
- di cambiamenti organizzativi della struttura organizzativa o dei settori di attività dell'azienda.

L'aggiornamento deve essere effettuato in forma ciclica e continuativa e il compito di disporre e porre in essere l'aggiornamento o l'adeguamento del Modello è attribuito al CdA.

Più in particolare:

1. l'OdV comunica al CdA ogni informazione della quale sia a conoscenza che possa determinare l'opportunità di procedere a interventi di aggiornamento del Modello
2. il programma viene predisposto dall'OdV con il contributo delle funzioni aziendali competenti e del Responsabile del Modello Organizzativo

3. i risultati del programma, e il progressivo stato avanzamento lavori, sono sottoposti, con scadenze predefinite, al CdA che dispone l'attuazione delle azioni di aggiornamento o di adeguamento
4. l'OdV provvede a monitorare l'attuazione delle azioni disposte e informa il CdA dell'esito delle attività.

# 3 PRINCIPI INTEGRATIVI AL CODE OF ETHICS ONTEX

## 3.1 Principi generali

Il raggiungimento degli obiettivi della SERENITY è perseguito, da parte di tutti coloro che operano nelle Società, con lealtà, serietà, onestà, competenza e trasparenza, nell'assoluto rispetto delle leggi e delle normative vigenti.
SERENITY adotta un comportamento socialmente responsabile, monitorando e rispondendo alle attese economiche di tutti i portatori di interesse (stakeholder), consapevoli del fatto che essi esigono un impegno quotidiano e credibile, frutto di una precisa politica manageriale e di un sistema aziendale organizzato a tal fine.

La Società ha ritenuto opportuno e necessario adottare ed emanare il presente documento che espliciti i valori, inclusi quelli già contenuti nel Code of Ethics e nel Codice di Condotta fornitori Ontex, a cui tutti i propri amministratori, dipendenti e collaboratori a vario titolo devono adeguarsi, accettando responsabilità, assetti, ruoli e regole della cui violazione, anche se da essa non consegue alcuna responsabilità aziendale verso terzi, essi assumono la personale responsabilità verso l'interno e verso l'esterno dell'azienda.

La conoscenza e l'osservanza di tali documenti da parte di tutti coloro che prestano attività lavorativa in SERENITY sono dunque condizioni primarie per la trasparenza e la reputazione della società. Inoltre il Code of Ethics e la presente Parte Generale sono portate a conoscenza di tutti coloro con i quali SERENITY intrattiene rapporti d'affari.

La vigilanza sull'attuazione del Code of Ethics e della presente Parte Generale nonché sulla sua applicazione è compito degli amministratori e dei dipendenti di SERENITY che ne segnalano le eventuali inadempienze o mancata applicazione all'OdV (persona di fiducia locale citata nel Code of Ethics).
La verifica sulla attuazione della presente Parte Generale e sulla sua applicazione è di competenza del CdA.
E' compito del CdA aggiornare il presente documento al fine di adeguarlo alla eventuale nuova normativa rilevante ed alla evoluzione della sensibilità civile, nonché farsi promotore per la richiesta degli adeguamenti del Code of Ethics verso il CEO Ontex.

Oltre a chiedere agli amministratori, ai dipendenti e a tutti i collaboratori interni ed esterni che a qualsiasi titolo forniscono la loro attività per SERENITY, di rispettarlo ed applicarlo scrupolosamente, si chiede che diventi una convinta adesione ad una filosofia di gestione ed operatività.
Per quanto sopra, il presente documento insieme al Code of Ethics viene diffuso all'interno di SERENITY e distribuito, insieme al Codice di Condotta Fornitori, a tutti i soggetti terzi che entrano in rapporto di affari con essa e pertanto:

- è nella responsabilità di ciascun Destinatario consultare il proprio superiore per qualsiasi chiarimento relativo all'interpretazione o all'applicazione delle regole di comportamento contenute nel presente documento e nel Code of Ethics, o in altre direttive emesse dalle competenti funzioni di SERENITY
- le regole contenute nel presente documento e nel Code of Ethics integrano il comportamento che i Destinatari, tra cui i dipendenti, devono osservare in conformità alle regole di ordinaria diligenza, anche ai sensi degli articoli del Codice Civile in materia di rapporti di lavoro (art. 2104 e 2105 c.c.)

- la mancata osservanza delle regole e delle direttive emesse può danneggiare SERENITY, che vigila sulla loro effettiva osservanza adottando all'uopo adeguate misure disciplinari nei confronti dei Destinatari che ne fossero responsabili, secondo quanto previsto dal sistema disciplinare adottato
- i Destinatari sono tenuti alla rigorosa osservanza del presente documento e del Code of Ethics in quanto la mancata osservanza costituisce violazione al "Modello di organizzazione, gestione e controllo" adottato ai sensi dell'art. 6 del D. Lgs. 231/01.

In nessun modo, la convinzione di agire a vantaggio di SERENITY, giustificherà l'adozione di comportamenti in contrasto con i principi del presente documento.

Nei prossimi paragrafi sono riportati i valori e comportamenti da seguire evidenziati dall'analisi rischi-reati della società SERENITY e non inclusi nel Code of Ethics.

## 3.2 Valore delle risorse umane

Il riconoscimento di aumenti salariali o di altri strumenti d'incentivazione (laddove presenti) e legge e dal contratto collettivo di lavoro, ai meriti individuali dei dipendenti, tra i quali la capacità di esprimere comportamenti e competenze organizzative improntati ai principi etici di riferimento della Società, indicati dal Code di Ethics e dal presente documento.

Il valore riconosciuto dall'azienda per le risorse umane appartenenti alla propria organizzazione e a quelle di terze parti tiene conto in maniera esplicita del sostegno alla lotta all'istigazione ed all'incitamento al razzismo ed alla xenofobia. A tal proposito l'azienda mette in atto tutte le possibili azioni di natura organizzativa, amministrativa e tecnica per evitare qualsiasi tipo di situazione compromettente in tal senso.

## 3.3 Divieto di falsi nummarii

SERENITY è contraria a qualsiasi forma di attività che possa ricondursi alla realizzazione dei reati di falso nummario, previsti dagli artt. 453 e ss. del codice penale.

Anche al fine di prevenire danni d'immagine alla società, è quindi vietato ai Destinatari del presente documento:

- effettuare contraffazioni di monete nazionali/straniere aventi corso legale nello Stato fuori dello Stato
- alterare in qualsiasi modo delle monete genuine per dare ad esse l'apparenza di un valore superiore
- acquistare o ricevere dal falsificatore o dall'alteratore ovvero da un intermediario delle monete contraffatte o alterate al fine di metterle in circolazione
- alterare monete nazionali o straniere aventi corso legale nello Stato o fuori dello Stato scemandone il valore
- acquistare o detenere monete contraffatte o alterate al fine di metterle in circolazione
- spendere o mettere in circolazione monete contraffatte o alterate, anche se ricevute in buona fede
- effettuare contraffazioni o alterazioni di valori di bollo
- introdurre nel territorio dello Stato, acquistare, detenere o mettere in circolazione valori di bollo contraffatti
- effettuare contraffazioni della carta filigranata che si adopera per la fabbricazione delle carte di pubblico credito o dei valori di bollo
- acquistare, detenere o alienare della carta filigranata di cui sopra contraffatta

- fabbricare, acquistare, detenere o alterare filigrane, programmi informatici o strumenti destinati esclusivamente alla alterazione o contraffazione di monete, valori di bollo e carta filigranata.

## 3.4 Utilizzo dell'accesso aziendale alla rete Internet

SERENITY si impegna ad evitare l'utilizzo dell'accesso aziendale alla rete Internet per motivi non strettamente attinenti alle ragioni lavorative e, in particolare, ne vieta l'utilizzo per venire in possesso di o distribuire materiale pornografico (in particolar modo se relativo a minori di anni diciotto).

Conseguentemente, anche al fine di evitare lesioni all'immagine della società ai Destinatari è comunque vietato di accedere a siti Internet che espongano materiale pornografico.

## 3.5 Divieto di attività terroristiche o eversive dell'ordine democratico

SERENITY è contraria a qualsiasi forma di attività realizzata con finalità di terrorismo o di eversione dell'ordine democratico.

Pertanto, anche al fine di evitare lesioni all'immagine della società:

- è vietato ai Destinatari del presente documento compiere qualsiasi forma di attività che abbia finalità di terrorismo o di eversione dell'ordine democratico
- il Destinatario che abbia il fondato sospetto che un suo collega svolga attività con finalità di terrorismo o eversione dell'ordine democratico, deve darne comunicazione immediata alla autorità di pubblica sicurezza nonché all'Amministratore Delegato e all'OdV, che adotteranno ogni iniziativa per collaborare attivamente con la predetta autorità.

## 3.6 Risorse umane e politica dell'occupazione

### *3.6.1 Rapporto di lavoro*

Il personale è assunto con regolare contratto di lavoro; non è tollerata alcuna forma di lavoro irregolare. Alla costituzione del rapporto di lavoro ogni collaboratore riceve accurate informazioni relative a:

- caratteristiche della funzione e delle mansioni da svolgere
- elementi normativi e livelli minimi retributivi, come regolati dal contratto collettivo nazionale di lavoro
- norme e procedure da adottare al fine di evitare i possibili rischi per la salute associati all'attività lavorativa
- presentazione del Modello Organizzativo, dei processi e delle procedure aziendali
- presentazione dei principi etici della società.

Tali informazioni sono presentate al collaboratore in modo che l'accettazione dell'incarico sia basata su un'effettiva comprensione. In ogni caso, il personale accetta formalmente il Code of Ethics, il presente documento ed il Sistema Disciplinare e Sanzionatorio adottato da SERENITY, nonché rende disponibilità per partecipare ad eventi di carattere formativo che l'azienda organizzerà (con particolare attenzione alla materia della responsabilità amministrativa d'impresa ed alla salute e sicurezza sui luoghi di lavoro).

### *3.6.1 Gestione del personale*

La Società evita qualsiasi forma di discriminazione nei confronti dei propri collaboratori.

Nell'ambito dei processi di gestione e sviluppo del personale, così come in fase di selezione, le decisioni prese sono basate sulla corrispondenza tra profili attesi e profili posseduti dai collaboratori.

L'accesso a ruoli e incarichi è anch'esso stabilito in considerazione delle competenze e delle capacità; inoltre, compatibilmente con l'efficienza generale del lavoro, sono favorite quelle flessibilità nell'organizzazione del lavoro che agevolano la gestione dello stato di genitorialità e in generale della cura dei figli.

La valutazione dei collaboratori è effettuata in maniera allargata coinvolgendo i responsabili e, per quanto possibile, i soggetti che sono entrati in relazione con il valutato.

I responsabili utilizzano e valorizzano pienamente tutte le professionalità presenti nella struttura mediante l'attivazione delle leve disponibili per favorire lo sviluppo e la crescita dei propri collaboratori.

In quest'ambito, riveste particolare importanza la comunicazione da parte dei responsabili dei punti di forza e di debolezza del collaboratore, in modo che quest'ultimo possa tendere al miglioramento delle proprie competenze anche attraverso una formazione mirata.

La formazione è assegnata a gruppi o a singoli collaboratori sulla base di specifiche esigenze di sviluppo professionale. Ogni responsabile è tenuto a valorizzare il tempo di lavoro dei collaboratori richiedendo prestazioni coerenti con l'esercizio delle loro mansioni.

Costituisce abuso della posizione di autorità richiedere, come atto dovuto al superiore gerarchico, prestazioni, favori personali o qualunque comportamento che configuri una violazione del presente documento e del Code of Ethics.

È assicurato il coinvolgimento dei Dipendenti e Collaboratori nello svolgimento del lavoro, anche prevedendo momenti di partecipazione a discussioni e decisioni funzionali alla realizzazione degli obiettivi aziendali. L'ascolto dei vari punti di vista, compatibilmente con le esigenze aziendali, consente al responsabile di formulare le decisioni finali; il collaboratore deve, comunque, sempre concorrere all'attuazione delle attività stabilite.

Qualsiasi dipendente di SERENITY che venga a conoscenza della circostanza che sono stati posti in essere comportamenti contrastanti con i principi che ispirano il presente documento o comunque in violazione degli obblighi imposti con il Modello Organizzativo ex D.Lgs.231/01, deve darne informazione tempestiva al proprio superiore gerarchico.

# 4 ORGANIZZAZIONE AZIENDALE

…omissis…

# 5 L'ORGANISMO DI VIGILANZA (ODV)

## 5.1 I requisiti

I requisiti che l'OdV, in quanto tale, deve possedere e che devono caratterizzare la sua azione sono i seguenti:

a) Autonomia e indipendenza

Al fine sia di garantire all'OdV piena autonomia di iniziativa e sia di preservarlo da qualsiasi forma di interferenza e/o di condizionamento, è previsto che l'Organismo:

- sia privo di compiti operativi e non ingerisca in alcun modo nella operatività della Azienda, affinché non sia compromessa la sua obiettività di giudizio
- nell'ambito dello svolgimento della propria funzione, sia organismo autonomo e indipendente non soggetto al potere gerarchico e disciplinare di alcun organo o funzione societaria
- riporti direttamente al CdA
- determini la sua attività e adotti le sue decisioni senza che alcuna delle funzioni aziendali possa sindacarle

b) Professionalità

Ai fini di un corretto ed efficiente svolgimento dei propri compiti, è essenziale che l'OdV garantisca una adeguata professionalità, intesa quest'ultima come insieme delle conoscenze, degli strumenti e delle tecniche necessarie per lo svolgimento dell'attività assegnata, sia di carattere ispettivo che consulenziale.

Sotto tale aspetto, assume rilevanza sia la conoscenza delle materie giuridiche, ed in particolare della struttura e delle modalità di commissione dei reati di cui al Decreto, e sia una adeguata competenza in materia di auditing e controlli aziendali, ivi incluso per ciò che attiene le tecniche di analisi e valutazione dei rischi, le metodologie connesse al flow charting di procedure e processi per l'individuazione dei punti di debolezza della struttura aziendale, le tecniche di intervista ed elaborazione dei risultati.

c) Continuità di azione

Per poter garantire una efficace e costante attuazione del Modello, l'OdV è un organismo dedicato esclusivamente ed a tempo pieno allo svolgimento dei compiti assegnati, senza quindi attribuzione di altre funzioni, ed è dotato di un adeguato budget e risorse adeguate

d) Onorabilità ed assenza di conflitti di interessi

Le regole definite nei prossimi paragrafi assumono carattere generale per la gestione dell'OdV. E' compito dell'OdV stesso dotarsi di un regolamento interno che sia specifico per tutte le attività continuative di operatività: programmazione incontri, modalità di convocazione e verbalizzazione, etc.

## 5.2 Composizione, nomina e durata.

L'OdV è un organo collegiale, costituito da tre membri, uno dei quali con funzione di Presidente eletto al suo interno. La composizione dell'OdV è determinata da specifico verbale del CdA, con indicazioni di nominativi, requisiti professionali e competenze specifiche.

I membri dell'OdV sono dotati, da un lato, di elevate e consolidate competenze giuridiche (specie di natura societaria, giuslavorista e penale), sistemiche ed in tema di attività ispettiva e consulenziale, dall'altro lato, di assoluta onorabilità, autonomia ed indipendenza. Tali competenze si ritengono essenziali per poter svolgere l'attività di verifica sul Modello; l'aspetto "consulenziale" si ritiene necessario in quanto l'OdV è chiamato anche a "formare" ed "informare" le altre funzioni, nonché tutti i dipendenti e collaboratori, circa l'esistenza del Modello e delle relative procedure: tale approccio è da intendersi in senso "consulenziale".

…omissis…

Al fine di svolgere le attività previste dall'art. 6, comma 1, D.Lgs. 231/01, l'OdV si avvale della collaborazione continuativa di uno staff di controllo interno dell'azienda, coordinato dal Responsabile del Modello Organizzativo, così da potere ricevere il più adeguato flusso di informazioni (campionamenti statistici, analisi e valutazione dei rischi, consulenza nell'individuazione delle regole di prevenzione dei rischi o nella predisposizione di meccanismi burocratici di contrapposizione dei compiti, etc.) ed il supporto necessario per l'analisi di risk & control in self assessment del monitoraggio. Il team di supporto è individuato in modo puntuale nei Process Owner riportati nella mappa dei processi aziendali.

Qualora la complessità delle aree di rischio, nella struttura sistemica dei processi aziendali individuati in ONTEX MANUFACTURING ITALY, tagli trasversalmente alcuni dei suddetti processi, l'OdV può individuare e nominare un Process Owner dedicato all'area di rischio. Queste figure costituiscono un insieme di referenti fondamentali per la corretta esecuzione delle attività proprie dell'OdV, in grado di fornire corretti *feedback* sull'andamento dei processi e su eventuali criticità, essendo operativamente impegnati nei processi aziendali, nelle aree aziendali a rischio o persino in singole attività a rischio reato.

### 5.3 Cause di ineleggibilità e decadenza.

…omissis…

### 5.4 Funzioni e compiti dell'OdV

L'OdV svolge la sua attività in condizioni di **autonomia** e di **indipendenza**.
Le sue funzioni sono state approvate dal CdA con specifico verbale.

In conformità al disposto di cui all'art, 6, I comma del D.Lgs. 231/01, all'OdV è affidato il compito di vigilare sul funzionamento e l'osservanza del Modello e di curare il suo aggiornamento.
All'OdV è affidato il **compito** di:

1. *Verifica e vigilanza sul Modello*, ossia:
   - effettuare una costante ricognizione delle attività dell'azienda, allo scopo di monitorare ed eventualmente integrare le aree a rischio-reato, individuando le implementazioni e/o le integrazioni da apportare al Modello
   - verificare l'adeguatezza del Modello, ovvero la sua idoneità a prevenire il verificarsi di comportamenti illeciti, nonché ad evidenziarne l'eventuale realizzazione
   - verificare l'effettività del Modello, ovvero la rispondenza tra i comportamenti concreti e quelli formalmente previsti dal Modello stesso
   - vigilare sulla congruità del sistema delle procure, al fine di garantire l'efficacia del modello; a questo scopo, può svolgere controlli incrociati per verificare la corrispondenza tra i poteri formalmente conferiti e le funzioni effettivamente svolte
   - vigilare sull'osservanza delle prescrizioni del Modello da parte dei destinatari, segnalando tempestivamente eventuali violazioni o tentativi di violazione ai vertici aziendali

- monitorare l'attività aziendale, nonché la funzionalità del complessivo sistema preventivo adottato dall'azienda con riferimento al settore della salute e della sicurezza sul lavoro e della gestione ambientale, effettuando verifiche periodiche e straordinarie (cd. "spot"), nonché i relativi follow-up
- collaborare fattivamente con FDC ai sensi delle procedure ISO 37001 istituite e rese attive nell'organizzazione

2. *Aggiornamento del Modello*, ossia:
   - curare l'aggiornamento del Modello, proponendo, se necessario, al CdA o alle funzioni aziendali eventualmente competenti l'adeguamento dello stesso, con il supporto del Responsabile del Modello Organizzativo, al fine di migliorarne l'adeguatezza e l'efficacia, anche in considerazione di eventuali sopraggiunti interventi normativi e/o di variazioni della struttura organizzativa o dell'attività aziendale e/o di riscontrate significative violazioni del Modello
   - esaminare le relazioni periodiche e le altre segnalazioni che prospettino eventuali violazioni del Modello, allo scopo di individuare possibili carenze nel suo funzionamento, proponendo le necessarie modificazioni; in tal caso, l'OdV avverte, senza ritardo, i vertici aziendali
   - verificare periodicamente il Modello organizzativo, prevedendo l'analisi ed il controllo di specifiche aree di attività aziendale ritenute a rischio. Nel corso dell'anno inoltre, al fine di confermare la validità del Modello, aggiorna la lista delle aree aziendali a rischio reato. Sulla base di tali verifiche verrà predisposto un rapporto da presentare al CdA dell'azienda che evidenzi le problematiche riscontrate ed eventualmente suggerisca le azioni correttive da intraprendere

3. *Informazione e formazione* sul Modello, ossia:
   - promuovere e monitorare le iniziative dirette a favorire la diffusione del Modello presso tutti i soggetti tenuti al rispetto delle relative previsioni (i "Destinatari")
   - promuovere e monitorare le iniziative, ivi inclusi i corsi e le comunicazioni, volte a favorire un'adeguata conoscenza del Modello da parte di tutti i Destinatari
   - riscontrare con la opportuna tempestività, anche mediante la predisposizione di appositi pareri, le richieste di chiarimento e/o di consulenza provenienti dalle funzioni o risorse aziendali ovvero dagli organi amministrativi e di controllo, qualora connesse e/o collegate al Modello

4. *Gestione dei flussi informativi da e verso l'OdV*, ossia:
   - assicurare il puntuale adempimento, da parte dei soggetti interessati, di tutte le attività di reporting inerenti il rispetto del Modello
   - esaminare e valutare tutte le informazioni e/o le segnalazioni ricevute e connesse al rispetto del Modello, ivi incluso per ciò che attiene le sospette violazioni dello stesso
   - informare gli organi competenti, nel proseguo specificati, in merito all'attività svolta, ai relativi risultati ed alle attività programmate
   - segnalare agli organi competenti, per gli opportuni provvedimenti, le eventuali violazioni del Modello ed i soggetti responsabili, proponendo la sanzione ritenuta più opportuna rispetto al caso concreto
   - in caso di controlli da parte di soggetti istituzionali, ivi inclusa la Pubblica Autorità, fornire il necessario supporto informativo agli organi ispettivi
   - gestire una comunicazione bidirezionale con FDC in merito ad aspetti di natura corruttiva sia effettiva che potenziale

…omissis…

## 5.5 Garanzie dell'OdV

…omissis…

## 5.6 Organismo di Vigilanza: obblighi

…omissis…

## 5.7 I flussi informativi che interessano l'Organismo di vigilanza

L'art. 6, II comma, lett. d) del D.Lgs. 231/01, dispone che il Modello deve prevedere obblighi di informazione nei confronti dell'OdV, in modo che lo stesso possa espletare al meglio la propria attività di verifica.

### *5.7.1 Flussi informativi verso l'Organismo di Vigilanza.*

Fatta salva la disciplina relativa agli obblighi informativi in relazione al compimento delle attività a rischio-reato, devono essere obbligatoriamente e tempestivamente trasmesse all'OdV da parte di tutti i Destinatari, vale a dire gli amministratori, i sindaci, i soggetti che operano per la società di revisione, nonché dai suoi dipendenti, inclusi i dirigenti, senza alcuna eccezione, ed ancora da tutti coloro che, pur esterni all'azienda, operino, direttamente o indirettamente, per SERENITY (es. procuratori, collaboratori a qualsiasi titolo, consulenti, fornitori, partner) di qualsiasi notizia relativa all'esistenza di possibili violazioni dei principi contenuti nel Modello.

I Destinatari (ivi compreso FDC), in particolare, devono segnalare all'OdV le notizie relative alla commissione o alla potenziale commissione di reati o di deviazioni comportamentali rispetto ai principi ed alle prescrizioni contenuti nel Modello. I Responsabili di Funzione/ Process Owner devono, inoltre, ed in particolare, segnalare le violazioni del Modello commesse dai dipendenti che a loro rispondono gerarchicamente.

Oltre a tutte le comunicazioni da effettuare nei confronti dell'OdV riportate in questa sede, si devono considerare anche i flussi di comunicazione dettati dalle diverse parti speciali in allegato, come definito nei paragrafi relativi protocolli specifici o nei controlli dell'OdV

Devono essere oggetto di segnalazione le seguenti informative:

- le segnalazioni e/o i provvedimenti aventi ad oggetto l'esistenza di un procedimento penale, relativi a fatti di interesse per l'azienda; come pure le segnalazioni concernenti richieste di assistenza legale inoltrate dal personale all'azienda per l'avvio di procedimenti penali
- le segnalazioni riguardanti altresì le controversie amministrative, civili o giuslavoristiche comunque riferibili ad aree di attività esposte al rischio-reato
- le segnalazioni, provenienti dal personale dell'azienda, comunque qualificato, relative alla commissione o al pericolo di commissione di reati o di violazioni delle prescrizioni del Modello; tali segnalazioni, anche in forma anonima, potranno essere inoltrate in forma scritta o per posta elettronica sul corrispondente indirizzo aziendale dell'OdV (alla stregua di un canale all'uopo dedicato) e gli autori delle segnalazioni andranno garantiti contro qualsiasi forma di ritorsione, discriminazione o penalizzazione, anche assicurando la riservatezza della loro identità
- le segnalazioni di FDC inerenti aspetti di natura corruttiva

…omissis…

Le informazioni acquisite dall'OdV saranno trattate in modo tale da garantire:

a) il rispetto della persona, della dignità umana e della riservatezza e da evitare per i segnalanti qualsiasi forma di ritorsione, penalizzazione o discriminazione, nonché

b) la tutela dei diritti di enti e persone in relazione alle quali sono state effettuate segnalazioni in mala fede e successivamente risultate infondate

L'OdV si è dotato di canali informativi dedicati (anche di specifico **indirizzo mail** debitamente istituito, comunicato e pubblicato in tutte le forme possibili), a garanzia di riservatezza per tutti i segnalanti, fisicamente esterni alla rete intranet aziendale, al fine di evitare accessi non consentiti, di qualsiasi natura, ai dati ed alle segnalazioni.

L'OdV valuta le segnalazioni ricevute con discrezionalità e responsabilità. A tal fine può ascoltare l'autore della segnalazione e/o il responsabile della presunta violazione, motivando per iscritto la ragione dell'eventuale autonoma decisione a non procedere.

…omissis…

# 6 GESTIONE DELLA DOCUMENTAZIONE E DELLA COMUNICAZIONE

…omissis…

# 7 WHISTLEBLOWING

## 7.1 Contesto normativo

Il D.Lgs. n. 165/2001, con l'art. 54-bis , prevede la tutela per il lavoratore - dipendente pubblico - che segnali un illecito o violazione ai soggetti preposti (whistleblowing), proteggendolo contro le eventuali ritorsioni da parte di colleghi o superiori.

La Legge n. 179 del 30 novembre 2017 avente ad oggetto "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato":

- ha modificato l'art. 54-bis del D.Lgs. 30 marzo 2001 n.165 relativo alla "Tutela del dipendente pubblico che segnala illeciti"
- ha modificato l'articolo 6 del D.Lgs 8 giugno 2001, n. 231, comma 2-bis relativo alla "Tutela del dipendente o collaboratore che segnala illeciti nel settore privato"
- ha "integrato la disciplina dell'obbligo di segreto d'ufficio, aziendale, professionale, scientifico e industriale".

## 7.2 Finalità della procedura

In riferimento alla propria Policy di Speak-up, SERENITY si impegna a rimuovere i fattori che possono ostacolare o disincentivare le segnalazioni che rivelino situazioni di corruzione o pregiudizievoli per l'organizzazione. In tale prospettiva, l'obiettivo perseguito è quello di fornire al whistleblower chiare indicazioni operative circa l'oggetto, i contenuti, i destinatari e le modalità di trasmissione delle segnalazioni, nonché in merito alle forme di tutela, sotto elencate, che gli vengono offerte dalla normativa in essere:

- tutela dell'anonimato
- sottrazione della segnalazione al diritto d'accesso
- divieto di discriminazione nei confronti del segnalante.

## 7.3 Oggetto della segnalazione

Possono essere oggetto della segnalazione non solo fatti tali da configurare fattispecie di reato, ma ogni situazione in cui, a prescindere dalla rilevanza penale, viene in evidenza un malfunzionamento della società. In particolare la segnalazione può riguardare azioni od omissioni, commesse o tentate, che siano:

- penalmente rilevanti
- poste in essere in violazione del Codice di comportamento dei dipendenti o di altre disposizioni sanzionabili in via disciplinare
- suscettibili di arrecare un pregiudizio patrimoniale alla SERENITY, ai suoi soci o a terzi
- suscettibili di arrecare un pregiudizio all'immagine della SERENITY o di terzi
- suscettibili di arrecare un pregiudizio ai dipendenti o ad altri soggetti che svolgono la loro attività presso la SERENITY
- suscettibili di arrecare un pregiudizio alla collettività in relazione all'azione della SERENITY.

La segnalazione non può invece riguardare lamentele o rimostranze di carattere personale del segnalante, o richieste che attengono alla disciplina del rapporto di lavoro o ai rapporti con il superiore gerarchico o i colleghi, per le quali occorre fare riferimento al servizio competente per la gestione del personale.

Il segnalante deve fornire tutti gli elementi utili alla ricostruzione del fatto volti ad accertare la fondatezza di quanto segnalato. In particolare la segnalazione deve contenere, tra l'altro, i seguenti elementi:

- generalità, qualifica o posizione professionale, sede di servizio e recapiti del segnalante
- circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione
- descrizione del fatto
- generalità o altri elementi che consentano di identificare il soggetto o i soggetti che hanno posto in essere i fatti segnalati
- eventuali altri soggetti che possono riferire sui fatti oggetto di segnalazione ed eventuali documenti che possono confermare la fondatezza di tali fatti
- ogni altra informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

E' indispensabile che i fatti siano conosciuti direttamente dal segnalante e non riportati o riferiti da altri soggetti. La segnalazione deve essere sottoscritta con firma autografa dal segnalante se cartacea, o con firma elettronica se si utilizza il sistema informatico o anche con mail specifica che identifichi il segnalante.

Le segnalazioni anonime, vale a dire prive di elementi che consentano di identificarne l'autore, anche se recapitate tramite le modalità previste dal presente documento, non verranno prese in considerazione a meno che siano relative a fatti di particolare gravità ed il loro contenuto risulti adeguatamente dettagliato e circostanziato.

### 7.4 Trasmissione della segnalazione.

La segnalazione può essere inviata attraverso due modalità:

- Analogica: la segnalazione con firma autografa, deve essere inserita in una doppia busta chiusa che rechi all'esterno la dicitura "riservata/personale" ed inviata alla SERENITY, che provvederà ad inoltrarla all'OdV
- Digitale: la segnalazione avviene tramite mail diretta all'OdV.

### 7.5 Contenuto della segnalazione

La segnalazione deve contenere tutte le informazioni indicate come obbligatorie per circoscrivere il problema, alimentando i campi del format sia informatico che cartaceo. La segnalazione può essere di tre tipi:

- Aperta: il segnalante solleva apertamente un problema senza limiti legati alla propria riservatezza
- Confidenziale: il nome del segnalante è conosciuto, ma l'organizzazione tratta la segnalazione in maniera riservata senza rivelare l'identità del medesimo in assenza di un suo esplicito consenso
- Anonima: le generalità del segnalante non sono esplicitate né sono altrimenti individuabili.

### 7.6 Destinatari della segnalazione

La segnalazione può essere indirizzata all'OdV.

Qualora il whistleblower rivesta la qualifica di pubblico ufficiale, l'invio della segnalazione ai suddetti soggetti non lo esonera dall'obbligo di denunciare alla competente Autorità Giudiziaria i fatti ritenuti penalmente rilevanti e le ipotesi di danno erariale.

## 7.7 Compiti del destinatario della segnalazione

L'OdV, all'atto del ricevimento della segnalazione, provvede alla protocollazione riservata del documento ed avvia, con le dovute cautele e nel rispetto della massima riservatezza, la procedura interna per la verifica dei fatti descritti nella segnalazione, investendo le strutture competenti per lo svolgimento dell'attività necessaria ad accertare i fatti medesimi. Può, in tal senso, effettuare ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati, adottando le necessarie misure di riservatezza. L'OdV è chiamato a segnalare a FDC le eventuali evidenze in merito a eventi corruttivi ed FDC è tenuto in modo totale a garantire la riservatezza che è stata istituita con la presente procedura.

Nel caso in cui ritenga fondata la segnalazione, l'OdV la trasmette all'AD (se soggetto non coinvolto nella segnalazione) dopo avere oscurato la sottoscrizione e sostituito i dati identificativi del segnalante con opportuni codici. Il destinatario effettua le proprie valutazioni sulle eventuali iniziative da intraprendere, e provvede a:

- comunicare le risultanze dell'istruttoria dell'OdV entro 30 giorni dalla ricezione della segnalazione
- presentare denuncia all'Autorità Giudiziaria competente qualora sussistano i presupposti di legge.

L'OdV informa dell'esito il segnalante, con le opportune precauzioni a garanzia della sua tutela, e provvede ad adottare, o a proporre di adottare se la competenza è di altri soggetti, tutte le misure necessarie al ripristino della legalità.

## 7.8 Tutela del segnalante

L'identità del segnalante è protetta in ogni contesto. A partire dal momento della segnalazione: tutti coloro che ricevono o sono coinvolti, anche solo accidentalmente, nella gestione della segnalazione sono obbligati a tutelare la riservatezza di tale informazione. La violazione dell'obbligo di riservatezza è fonte di responsabilità disciplinare, fatte salve ulteriori forme di responsabilità previste dall'ordinamento. Nel caso in cui, a seguito della segnalazione, venga avviato un procedimento disciplinare, l'identità del segnalante può essere rivelata al titolare del potere disciplinare e all'incolpato in uno dei seguenti casi:

a.) qualora vi sia il consenso espresso del segnalante, sempre che la contestazione dell'addebito disciplinare risulti fondata su accertamenti distinti e ulteriori rispetto alla segnalazione

b.) qualora la contestazione dell'addebito disciplinare sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante risulti assolutamente indispensabile alla difesa dell'incolpato.

La tutela della riservatezza non può essere garantita nei casi in cui non è opponibile il segreto d'ufficio. La segnalazione è sottratta all'accesso civico e a quanto previsto dagli artt. 22 ss. della legge 241/1990. Per quanto riguarda il divieto di discriminazioni nei confronti del segnalante si evidenzia che:

a. tutti coloro che effettuano una segnalazione non possono essere sanzionati, licenziati o sottoposti ad alcuna misura discriminatoria per motivi collegati, anche solo indirettamente, alla segnalazione

b. il segnalante che ritiene di aver subito una discriminazione ne dà notizia circostanziata, anche tramite un'organizzazione sindacale, all'OdV che, valutatane la fondatezza, la segnala:

   · al responsabile di servizio di appartenenza dell'autore della presunta discriminazione, affinché valuti se adottare atti o provvedimenti volti a ripristinare la situazione e a rimediare agli effetti negativi della discriminazione, ovvero avviare un procedimento disciplinare

   • all'AD della SERENITY per le valutazioni di propria competenza.

## 7.9 Responsabilità del segnalante

La tutela del segnalante non può essere assicurata, e resta ferma la sua responsabilità, nel caso in cui la segnalazione configuri un'ipotesi di calunnia o diffamazione ai sensi del codice penale o un fatto illecito ai sensi dell'art. 2043 del codice civile.

Sono altresì fonte di responsabilità, in sede disciplinare e nelle altre competenti sedi, eventuali forme di abuso della presente procedura, quali le segnalazioni manifestamente opportunistiche e/o effettuate al solo scopo di danneggiare il denunciato o altri soggetti, e ogni altra ipotesi di utilizzo improprio o di intenzionale strumentalizzazione dell'istituto oggetto della presente procedura.

Qualora a seguito degli accertamenti interni, la segnalazione risulti manifestamente infondata ed effettuata per procurare a sé un vantaggio o al solo scopo di danneggiare il denunciato o altri soggetti, saranno valutate azioni di responsabilità disciplinare a carico del segnalante.

## 7.10 Sistema informatico per la gestione della segnalazione

Al fine da evitare che il dipendente ometta di segnalare condotte illecite per timore di subire misure discriminatorie, è opportuno che le società si dotino di un sistema che si componga di una parte organizzativa e di una parte tecnologicamente avanzata integrata con la precedente.

La parte organizzativa è stata esposta dettagliatamente nei paragrafi precedenti, mentre quella tecnologica prevedere la predisposizione di un sistema informatico che rilevi la segnalazione, tuteli la riservatezza del segnalatore e del segnalante, gestisca il flusso dei dati e delle informazioni all'interno dell'organizzazione, consenta al segnalante di verificare lo stato di avanzamento dell'istruttoria.

L'ANAC ha predisposto il sistema gestionale per la propria organizzazione e lo ha messo a disposizione, in modalità di riuso semplice, a tutte le società che ne faranno richiesta.

Si faccia diretto riferimento al sito dell'ANAC per l'adozione di tale procedura.

## 7.11 Riservatezza, gestione dei dati personali e sicurezza

Secondo quanto previsto dall'articolo 13 del Regolamento 679/2016, la SERENITY, in qualità di titolare del trattamento dei dati, è tenuta a fornire informazioni in merito all'utilizzo dei dati personali,. La raccolta dei dati personali viene effettuata registrando i dati forniti, in qualità di interessato, per le seguenti finalità:

a) accertamento di illeciti commessi da dipendenti della SERENITY
b) miglioramento dei processi amministrativi della SERENITY
c) prevenzione della corruzione nella SERENITY.

In relazione alle finalità descritte, il trattamento dei dati personali avviene mediante strumenti manuali o telematici con logiche strettamente correlate alle finalità sopra evidenziate e, comunque, in modo da garantire la sicurezza e la riservatezza dei dati stessi.

I dati personali potranno essere conosciuti da SERENITY, nonché dall'AD.

I regolamento 679/16 conferisce agli interessati il diritto di:

- ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano, anche se non ancora registrati, e la loro comunicazione in forma intelligibile
- ottenere l'indicazione:
  a) dell'origine dei dati personali
  b) delle finalità e delle modalità del trattamento
  c) della logica applicata in caso di trattamento effettuato con l'ausilio di strumenti elettronici
  d) degli estremi identificativi del titolare, dei responsabili e del rappresentante designato
  e) dei soggetti o delle categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di rappresentante designato nel territorio dello Stato, di responsabili o incaricati.

L'interessato ha diritto, inoltre, di ottenere:

a) l'aggiornamento, la rettificazione ovvero, quando vi ha interesse, l'integrazione dei dati

b) la cancellazione, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati

c) l'attestazione che le operazioni, di cui alle lettere a) e b), sono state portate a conoscenza, anche per quanto riguarda il loro contenuto, di coloro ai quali i dati sono stati comunicati o diffusi, eccetto il caso in cui tale adempimento si riveli impossibile o comporti un impiego di mezzi manifestamente sproporzionato rispetto al diritto tutelato.

L'interessato ha diritto di opporsi, in tutto o in parte:

a) per motivi legittimi al trattamento dei dati personali che lo riguardano, ancorché pertinenti allo scopo della raccolta;

b) al trattamento di dati personali che lo riguardano a fini di invio di materiale pubblicitario o di vendita diretta o per il compimento di ricerche di mercato o di comunicazione commerciale.

# 8 MAPPATURA DEI RISCHI

…omissis…

## 8.1 Principi generali validi per la prevenzione dei reati

**COSA E' OBBLIGATORIO**

Tutto il personale è tenuto a conformarsi ai seguenti PRINCIPI GENERALI:

- Rigoroso rispetto di tutte le disposizioni normative e legislative nazionali e sovranazionali, nonché di tutte le regole interne al sistema di governance della SERENITY S.p.A. che disciplinano l'attività aziendale, con particolare riferimento alle disposizioni di contrasto o di prevenzione di reati presupposto ricadenti nell'ambito applicativo del D. lgs 231/01 e s.m.i.
- Immediata segnalazione all'OdV di qualsiasi soggetto correlato a SERENITY S.p.A. e di qualsiasi comportamento ad essa imputabile che destino il sospetto di una collusione con o di un coinvolgimento in attività di reato presupposto
- Instaurazione e mantenimento di qualsiasi rapporto o contatto con soggetti od organizzazioni esterne, secondo criteri di massima prudenza e trasparenza, previa in ogni caso assunzione di tutte le informazioni disponibili ed utili sul conto di tali soggetti ed organizzazioni
- Nei rapporti con le Pubbliche Autorità, con particolare riguardo alle Autorità giudicanti ed inquirenti, mantenimento di un comportamento chiaro, trasparente, diligente e collaborativo, mediante la comunicazione di tutte le informazioni, i dati e le notizie eventualmente richieste
- Inserimento, nei contratti con i Fornitori, i Collaboratori esterni e i Partner, di un'apposita dichiarazione dei medesimi con cui si affermi:

a) di essere a conoscenza della normativa di cui al D.Lgs 231/01 e delle sue implicazioni per SERENITY S.p.A., nonché dell'adozione da parte della stessa del Modello e del Codice etico
b) di non essere mai stati implicati in procedimenti giudiziari relativi ai reati contemplati nel D.Lgs 231/01 (o se lo sono stati, devono comunque dichiararlo ai fini di una maggiore attenzione da parte dell'azienda in caso si addivenga all'instaurazione del rapporto di consulenza o partnership)
c) di impegnarsi al rispetto delle prescrizioni contenute nel Decreto, nonché dei principi contenuti nel Modello e nel Codice etico
d) di essere consapevoli circa le conseguenze della violazione da parte degli stessi delle norme di cui al D.Lgs 231/01 nonché dei principi di cui al Modello (ad es., clausole risolutive espresse, penali)

Nello specifico, è obbligatorio anche:

REATI DI FEDE PUBBLICA (R2)

- Acquistare i valori di bollo esclusivamente presso le rivendite autorizzate

PER REATI SOCIETARI (R3)

- Rispettare tutte le disposizioni normative e legislative nazionali e sovranazionali, in tutte le attività finalizzate alla formazione del bilancio e delle altre comunicazioni sociali, al fine di fornire al socio ed ai terzi una informazione veritiera e corretta sulla situazione economica, patrimoniale e finanziaria della società
- Osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi in genere
- Assicurare il regolare funzionamento della Società e degli Organi Sociali, garantendo ed agevolando ogni forma di controllo interno sulla gestione sociale previsto dalla legge
- Osservare rigorosamente tutte le norme poste dalla legge a tutela dell'integrità ed effettività del capitale sociale, al fine di non ledere le garanzie dei creditori e dei terzi
- Garantire l'assoluta terzietà ed indipendenza dei revisori rispetto agli incaricati alla consulenza contabile e fiscale
- Verificare la corretta trascrizione dei verbali degli Organi sociali nei rispettivi libri dei verbali e verificarne la corretta sottoscrizione
- Effettuare con tempestività, correttezza e buona fede tutte le comunicazioni previste dalla legge e dai regolamenti nei confronti delle Autorità di Vigilanza, non frapponendo alcun ostacolo all'esercizio delle funzioni di vigilanza da queste esercitate
- Effettuare tutte le operazioni di rilevazione, valutazione e registrazione con correttezza e nel rispetto dei principi di prudenza, veridicità e completezza e, in generale, dei principi contabili nazionali ed internazionali
- Assicurare il controllo su tutti i flussi finanziari e i trasferimenti di beni o utilità di ammontare o valore rilevante con riferimento alle operazioni verso terzi; tali controlli devono, in particolare, tener conto della sede legale della società controparte, degli istituti di credito utilizzati e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie
- Assicurare il controllo su tutti i flussi di tesoreria; tali controlli devono, in particolare, riguardare il rispetto delle soglie per i pagamenti in contanti, l'eventuale utilizzo di libretti al portatore o anonimi per la gestione della liquidità, ecc.
- Prevedere un sistema informatico ad accesso limitato che consenta di tracciare i singoli passaggi e di identificare i soggetti che inseriscono i dati relativi ai flussi finanziari e ai trasferimenti di beni o utilità; gli atti e i documenti attinenti agli incassi e ai pagamenti effettuati, ivi inclusi i dati e le informazioni per l'alimentazione dell'applicativo di supporto alla fatturazione, dovranno, in particolare, essere resi accessibili agli organi di controllo e, in ogni caso, essere affidati in esclusiva a una funzione estranea alla gestione di altre fasi del rapporto

- Prevedere la separazione tra le funzioni titolari delle attività di gestione, impiego e controllo delle risorse finanziarie ovvero di beni e utilità
- Individuare specifiche condizioni e modalità d'impiego delle risorse finanziarie o di beni e utilità di ammontare o valore rilevante in modo che la funzione responsabile ne autorizzi l'impiego solo previa verifica dell'idonea documentazione giustificativa, oltre che della ricorrenza dei presupposti di ragionevolezza, necessità e legittimità
- Verificare il livello di adeguamento delle società collegate rispetto all'adozione di misure e controlli antiriciclaggio
- Verificare la regolarità dei pagamenti, con riferimento alla piena coincidenza tra destinatari/ordinanti dei pagamenti e controparti effettivamente coinvolte nelle transazioni
- Effettuare controlli formali e sostanziali dei flussi finanziari aziendali, con riferimento ai pagamenti verso terzi. Tali controlli devono tener conto della sede legale della società controparte (ad es. paradisi fiscali, Paesi a rischio terrorismo, ecc.), degli Istituti di credito utilizzati (sede legale delle banche coinvolte nelle operazioni e Istituti che non hanno insediamenti fisici in alcun Paese) e di eventuali schermi societari e strutture fiduciarie utilizzate per transazioni o operazioni straordinarie
- Non accettare pagamenti in contanti oltre i limiti previsti dal D.lgs. 231/07 e successive modifiche e integrazioni
- Non utilizzare strumenti anonimi per il compimento di operazioni di trasferimento di importi rilevanti
- Non trasferire denaro e titoli al portatore (assegni, vaglia postali, certificati di deposito, ecc.) per importi complessivamente superiori ai limiti di legge (12.500 euro, Legge 6 agosto 2008 n. 133), se non tramite intermediari a ciò abilitati, intesi quali banche, istituti di moneta elettronica e Poste Italiane S.p.A.
- Non accettare rapporti contrattuali con clienti o controparti contrattuali che abbiano sede o residenza ovvero qualsiasi collegamento con paesi considerati non cooperativi dal Gruppo di Azione Finanziaria contro il riciclaggio di denaro (GAFI)

REATI CONTRO LA PERSONALITA' INDIVIDUALE E LA PERSONA (R4)

- Nella selezione dei fornitori, e in particolare dei fornitori di particolari servizi (quali ad esempio le imprese di pulizia, le agenzie di viaggi, ecc.) è sempre necessario valutare con particolare attenzione l'affidabilità di tali partner ai fini della prevenzione dei reati di cui alla presente parte speciale, anche attraverso indagini ex ante (specie in relazione a particolari indicatori di rischio quali il costo della manodopera del fornitore, l'allocazione degli insediamenti produttivi, ecc.)

REATI AMBIENTALI (R5)

- Stretta osservanza delle leggi e del regolamenti che disciplinano le attività aziendali con particolare riferimento alle attività a rischio per i reati ambientali
- Stretta osservanza delle regole definite dal Codice Etico, dal presente Modello, dalle procedure e norme di comportamento Interne e, in particolare, delle norme e prassi operative definite dal Sistema di Gestione Ambientale della Società
- Redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni In materia ambientale ed a consentire un controllo efficace sul comportamenti e sulle attività della Società
- Immediata segnalazione di ogni situazione di violazione delle norme da parte di esponenti aziendali, consulenti o partner, ovvero di ogni situazioni di pericolo, reale o potenziale, In materia ambientale

- Inserimento di clausole rescissorie nei contratti di appalto che evidenzino la possibile immediata e unilaterale rescissione del contratto, in caso di gravi violazioni in materia ambientale commessi dalle ditte appaltatici e/o subappaltatici. Identificazione delle violazioni ritenute gravi ai fini della rescissione immediata suddetta
- Inserimento nei contratti con fornitori/ subappaltatori di modalità più specifiche di gestione degli aspetti indiretti ambientali
- Verbalizzazione delle decisioni prese in occasione di riunioni in tema ambientale

REATI DI TERRORISMO (R6)

- Instaurazione e mantenimento di qualsiasi rapporto o contatto con soggetti od organizzazioni esterni, particolarmente se insediati in Paesi ad elevato rischio terroristico, secondo criteri di massima prudenza e trasparenza, previa in ogni caso assunzione di tutte le informazioni disponibili ed utili sul conto di tali soggetti ed organizzazioni; per "Paesi ad elevato rischio terroristico" si intendono i Paesi di volta in volta qualificati tali dalle autorità nazionali di pubblica sicurezza e/o da organizzazioni internazionali cui l'Italia aderisca (es.: OCSE, ONU, NATO, ecc.)
- Immediata segnalazione all'OdV di qualsiasi soggetto correlato a SERENITY S.p.A. e di qualsiasi comportamento ad essa imputabile che destino il sospetto di una collusione con o di un coinvolgimento in attività od organizzazioni terroristico – eversive
- Nelle possibili alleanze e rapporti di fornitura con organizzazioni in Paesi a rischio, esecuzione di verifiche preventive per valutare il "rischio paese" ogni qualvolta la Società intenda intraprendere iniziative economiche/commerciali in determinate aree geografiche
- Richieste preventive di documentazione relativamente alla persona fisica o all'ente controparte (certificato casellario giudiziario, carichi pendenti, certificato camerale con dicitura antimafia, referenze qualificanti ecc.), anche in riferimento legali rappresentanti, ai membri del consiglio di amministrazione, direttori generali, soci di maggioranza. Ove non sia possibile una raccolta di documenti tali da poter verificare i c.d. requisiti di "moralità" della controparte (ad es. perché appartenente ad uno Stato in cui non vi siano certificazioni corrispondenti a quelle rilasciate in Italia) si dovranno assumere tutte le informazioni possibili al fine di valutarne l'affidabilità, assicurando la tracciabilità e la verificabilità delle stesse tramite apposita relazione scritta. Nel caso in cui la controparte sia una società, dovrà essere individuata la compagine azionaria di controllo risalendo fino alla capogruppo, nonché l'eventuale esistenza - sulle azioni della società in questione - di diritti reali di godimento o di garanzia con diritto di voto sulla base delle risultanze del Libro soci
- Nei contratti stipulati con partner commerciali/finanziari devono essere previste clausole che vietano la cessione del contratto o il subappalto. In mancanza di tali clausole si dovrà applicare lo standard di controllo relativo ai requisiti di moralità anche ai potenziali cessionari/subappaltatori. Nei contratti stipulati con partner commerciali/finanziari devono inoltre essere inserite clausole risolutive, con pagamento di congrua penale a carico della controparte, nel caso in cui vengano meno i richiesti requisiti di "moralità" ed anche nel caso di produzione di certificazioni/ informazioni non veritiere. Devono essere infine previsti, a carico della controparte, obblighi di comunicazione di variazioni nella propria composizione societaria successive alla stipulazione del contratto

- In fase di assunzione di personale, i criteri di selezione dei Dipendenti, fornitori, agenti, procacciatori d'affari ed altri collaboratori attuali e potenziali, soprattutto nei Paesi ad elevato rischio terroristico, devono prevedere la verifica preventiva e costante del possesso dei necessari requisiti di assoluta estraneità ad organizzazioni o ad attività di tipo terroristico - eversivo, integrità, lealtà e competenza. A tal fine, particolare rilevanza potranno avere le informazioni assunte tramite autorità di pubblica sicurezza ed agenzie specializzate, i controlli periodici delle liste dei sospettati di attività o collusioni terroristiche ufficialmente diramate da autorità nazionali e sovranazionali, il controllo delle referenze obbligatoriamente fornite dagli interessati, ecc.

REATI E ILLECITI AMMINISTRATIVI DI MARKET ABUSE (R7)

- Immediata segnalazione all'OdV di qualsiasi soggetto correlato a SERENITY S.p.A. e di qualsiasi comportamento ad essa imputabile che destino il sospetto di una collusione con o di un coinvolgimento in attività di reati amministrativi e di market abuse
- Mantenere riservati i documenti e le informazioni acquisiti nello svolgimento dei propri compiti e, in particolare, assicurare che la circolazione interna e verso Terzi di documenti contenenti informazioni potenzialmente privilegiate sia soggetta ad ogni necessaria attenzione e cautela, onde evitare pregiudizi e indebite divulgazioni
- Non comunicare ad altri, se non per motivi d'ufficio, le informazioni potenzialmente privilegiate di cui si viene a conoscenza
- Far sottoscrivere, ai Terzi cui si comunicano informazioni potenzialmente privilegiate, in occasione del conferimento dell'incarico, un impegno di riservatezza
- Instaurazione e mantenimento di qualsiasi rapporto o contatto con soggetti od organizzazioni esterni, particolarmente se insediati in Paesi a rischio, secondo criteri di massima prudenza e trasparenza, previa in ogni caso assunzione di tutte le informazioni disponibili ed utili sul conto di tali soggetti ed organizzazioni
- Immediata segnalazione all'OdV di qualsiasi soggetto correlato a SERENITY S.p.A. e di qualsiasi comportamento ad essa imputabile che destino il sospetto di commissione di reati transnazionali
- Richieste preventive di documentazione relativamente alla persona fisica o all'ente controparte (certificato casellario giudiziario, carichi pendenti, certificato camerale con dicitura antimafia, referenze qualificanti ecc.), anche in riferimento legali rappresentanti, ai membri del consiglio di amministrazione, direttori generali, soci di maggioranza. Ove non sia possibile una raccolta di documenti tali da poter verificare i c.d. requisiti di "moralità" della controparte (ad es. perché appartenente ad uno Stato in cui non vi siano certificazioni corrispondenti a quelle rilasciate in Italia) si dovranno assumere tutte le informazioni possibili al fine di valutarne l'affidabilità, assicurando la tracciabilità e la verificabilità delle stesse tramite apposita relazione scritta. Nel caso in cui la controparte sia una società, dovrà essere individuata la compagine azionaria di controllo risalendo fino alla capogruppo, nonché l'eventuale esistenza - sulle azioni della società in questione - di diritti reali di godimento o di garanzia con diritto di voto sulla base delle risultanze del Libro soci
- Nei contratti stipulati con partner commerciali/finanziari devono essere previste clausole che vietano la cessione del contratto o il subappalto. In mancanza di tali clausole si dovrà applicare lo standard di controllo relativo ai requisiti di moralità anche ai potenziali cessionari/subappaltatori. Nei contratti stipulati con partner commerciali/finanziari devono inoltre essere inserite clausole risolutive, con pagamento di congrua penale a carico della controparte, nel caso in cui vengano meno i richiesti requisiti di "moralità" ed anche nel caso di produzione di certificazioni/ informazioni non veritiere. Devono essere infine previsti, a carico della controparte, obblighi di comunicazione di variazioni nella propria composizione societaria successive alla stipulazione del contratto

- In fase di assunzione di personale, i criteri di selezione dei Dipendenti, fornitori, agenti, procacciatori d'affari ed altri collaboratori attuali e potenziali, devono prevedere la verifica preventiva e costante del possesso dei necessari requisiti di assoluta estraneità ad organizzazioni o ad attività criminali, integrità, lealtà e competenza. A tal fine, particolare rilevanza potranno avere le informazioni assunte tramite autorità di pubblica sicurezza ed agenzie specializzate, i controlli periodici delle liste dei sospettati di attività criminali segnalate, il controllo delle referenze obbligatoriamente fornite dagli interessati, ecc.
- Instaurazione e mantenimento di qualsiasi rapporto o contatto con soggetti od organizzazioni esterni, secondo criteri di massima prudenza e trasparenza, previa in ogni caso assunzione di tutte le informazioni disponibili ed utili sul conto di tali soggetti ed organizzazioni
- Immediata segnalazione all'OdV di qualsiasi soggetto correlato a SERENITY S.p.A. e di qualsiasi comportamento ad essa imputabile che destino il sospetto di commissione di reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita
- Nei contratti stipulati con partner commerciali/finanziari devono essere previste clausole che vietano la cessione del contratto o il subappalto. In mancanza di tali clausole si dovrà applicare lo standard di controllo relativo ai requisiti di moralità anche ai potenziali cessionari/subappaltatori. Nei contratti stipulati con partner commerciali/finanziari devono inoltre essere inserite clausole risolutive, con pagamento di congrua penale a carico della controparte, nel caso in cui vengano meno i richiesti requisiti di "moralità" ed anche nel caso di produzione di certificazioni/ informazioni non veritiere. Devono essere infine previsti, a carico della controparte, obblighi di comunicazione di variazioni nella propria composizione societaria successive alla stipulazione del contratto

REATI INFORMATICI (R10)

- Utilizzo delle informazioni, dei dati, dei programmi e dei sistemi informatici esclusivamente per le attività attinenti alla propria mansione ovvero ai compiti assegnati, astenendosi dall'utilizzare le apparecchiature informatiche in dotazione al di fuori delle autorizzazioni prescritte
- In caso di smarrimento o furto di apparecchiature informatiche aziendali, presentazione immediata della denuncia all'autorità giudiziaria preposta, informando tempestivamente il responsabile dei sistemi informatici ovvero il proprio responsabile
- Utilizzo della connessione a internet esclusivamente per lo svolgimento delle proprie mansioni ovvero dei compiti assegnati e per il tempo strettamente necessario
- Informazione immediata del responsabile dei sistemi informatici qualora si venga a conoscenza della password di un altro utente
- Segnalazione tempestiva di utilizzi e/o funzionamenti anomali dei sistemi informatici al responsabile dei sistemi informatici
- Osservazione di ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni della Società, in base a quanto previsto dalle politiche di sicurezza aziendale per la protezione e il controllo dei sistemi informatici
- Nella selezione dei fornitori, e in particolare dei fornitori di particolari servizi (quali ad esempio le imprese di pulizia, le agenzie di viaggi, ecc.) è sempre necessario valutare con particolare attenzione l'affidabilità di tali partner ai fini della prevenzione dei reati di cui alla presente parte speciale, anche attraverso indagini ex ante (specie in relazione a particolari indicatori di rischio quali il costo della manodopera del fornitore, l'allocazione degli insediamenti produttivi, ecc.)
- Nell'utilizzo delle risorse informatiche si applicano i criteri generali del codice etico e i protocolli specifici già validi per combattere i reati informatici
- Inventario delle attrezzature hardware, i programmi software e le licenze d'uso e controllo periodico di tale inventario, con conservazione dei programmi in luoghi idonei alla loro salvaguardia

- Previsione, per ciascun profilo aziendale o dipendente, delle password di accesso per i diversi sistemi informatici e telematici
- Registrazione degli accessi a internet e alle reti telematiche con monitoraggio della trasmissione e diffusione di dati

REATI CONTRO INDUSTRIA E COMMERCIO (R12)

- Nel controllo dei prodotti acquistati, accertare legittima provenienza dei prodotti acquistati, con particolare riferimento a quelli che, per la loro qualità o per l'entità del prezzo, inducano a ritenere che siano state violate le norme in materia di proprietà intellettuale, di origine o provenienza
- Nell'acquisizione/ sviluppo di applicativi informatici, verificare preliminarmente alla progettazione e sviluppo di prodotti o sistemi informatici e tecnologici l'eventuale esistenza di marchi registrati e di contenuti similari brevettati

REATI VIOLAZIONE DIRITTO D'AUTORE (R13)

- Monitorare le clausole di gestione di proprietà intellettuale in contratti e licenze di terzi: deve essere presente una fase di verifica di tali condizioni in fase di riesame dei contratti di acquisto per quanto riguarda modelli, prototipi, simulacri, documentazione tecnica o tecnologica, know–how, invenzioni, innovazioni, perfezionamenti, software, modelli di simulazione
- I contratti di acquisto prevedano che, in caso di contestazione da parte di terzi dell'uso di particolari prodotti progettati autonomamente dal partner/ fornitore, quest'ultimo provveda a tenere indenne e a manlevare la Società da ogni pretesa, danno e/o da qualsiasi provvedimento che possa limitare la produzione e/o la vendita del prodotto da parte della Società, nella misura che la stessa riterrà più opportuna
- I contratti di acquisto prevedano obblighi di riservatezza nei confronti del fornitore/partner, affinché tratti come confidenziali tutte le informazioni tecniche, ricevute dalla Società e non utilizzi, per attività diverse da quelle di cui all'accordo, informazioni di qualsiasi genere relative alle attività svolte, di cui venga a conoscenza durante il periodo di validità dell'accordo
- I contratti di acquisto prevedano apposite clausole che consentano alla Società o a persone/enti delegati dalla stessa, di effettuare ispezioni, verifiche e controlli dei processi produttivi, dei mezzi di produzione, dei metodi di lavorazione e/o di controllo e di collaudo utilizzati dallo stesso, ivi compreso, fra gli altri, ogni controllo e/o ispezione concernente l'adempimento di quanto previsto in tema di eventuale certificazione/ omologazione del prodotto
- Qualora si renda opportuno stipulare accordi di licenze d'uso attive e/o passive di marchi, dovranno essere definiti nei relativi contratti clausole e procedure che impediscano l'utilizzo delle suddette licenze in modo non conforme alle policy della società titolare o in violazione dei diritti di terze parti affinché:
  - sia previsto un termine per la scadenza dello smaltimento delle scorte di materiale ovvero di quei supporti sui quali il marchio sia stato apposto (inventory disposition)
  - il licenziante dichiari di non essere a conoscenza di eventuali contestazioni sul marchio e garantisca la sua legittima titolarità e che lo stesso non pregiudichi il diritto dei terzi
  - sia prevista la manleva e l'indennizzo da parte del licenziatario in caso di contestazioni di diritti di proprietà intellettuale, contraffazione, concorrenza sleale o qualsiasi violazione di diritti di terze parti
  - sia esplicitato, in caso di contestazione, il diritto di collaborazione stragiudiziale e giudiziale tra licenziante e licenziatario stabilendo i relativi diritti e/oneri
- Prevedere nei contratti di acquisto specifiche clausole di recesso e di risarcimento in caso di accertate violazioni in materia di proprietà industriale ovvero di accertate difformità rispetto alle caratteristiche dichiarate o pattuite di prodotti o opere dell'ingegno

- Prevedere l'acquisto diretto del prodotto dai titolari del marchio o brevetto ovvero l'acquisto da altri solo previa verifica della liceità di utilizzo del marchio o brevetto

REATI DI SALUTE E SICUREZZA (R14)

- Stretta osservanza delle leggi e del regolamenti che disciplinano le attività aziendali con particolare riferimento alle attività a rischio per i reati di sicurezza
- Stretta osservanza delle regole definite dal Codice Etico, dal presente Modello, dalle procedure e norme di comportamento Interne e, in particolare, delle norme e prassi operative definite dal Sistema di Gestione della Sicurezza della Società
- Attribuzione di responsabilità in materia di sicurezza e igiene sul lavoro, con particolare riferimento alle attribuzioni di compiti e doveri (rete di controllo de facto et de jure), alla verifica dei requisiti professionali dei soggetti preposti alla prevenzione/protezione, alle attività del Servizio Prevenzione e Protezione e del Servizio Sanitario
- Valutazione dei rischi, con elaborazione del documento di valutazione dei rischi (DVR),
- Informazioni specifiche e formazione ai lavoratori sui rischi legati alla sicurezza per le diverse mansioni
- Monitoraggio del sistema preventivo, con particolare riferimento alla verifica del rispetto degli standard tecnico–strutturali di legge relativi ad attrezzature, impianti, luoghi di lavoro, agenti chimici fisici e biologici, Verifica applicazione ed efficacia delle procedure adottate, Misure di mantenimento e miglioramento, Gestione comportamenti posti in essere violazione delle norme, provvedimenti disciplinari o altri interventi di tipo formativo, informativo e preventivo
- Redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni in materia sicurtale ed a consentire un controllo efficace sul comportamenti e sulle attività della Società
- Immediata segnalazione di ogni situazione di violazione delle norme da parte di esponenti aziendali, consulenti o partner, ovvero di ogni situazioni di pericolo, reale o potenziale, In materia di sicurezza
- Assegnazione di adeguate procure e deleghe a personale qualificato in riferimento ai vincoli del sistema di gestione della sicurezza; al titolare della procura, che deve essere persona di provate capacità ed esperienza in materia, devono essere riconosciuti poteri di spesa adeguati alle funzioni conferite, nonché poteri di sospensione dei lavoratori in caso si ravvisino situazioni di pericolo per la sicurezza
- Inserimento di clausole rescissorie nei contratti di appalto che evidenzino la possibile immediata e unilaterale rescissione del contratto, in caso di gravi violazioni in materia di sicurezza commessi dalle ditte appaltatici e/o subappaltatici. Identificazione delle violazioni ritenute gravi ai fini della rescissione immediata suddetta

REATI DI IMMIGRAZIONE CLANDESTINA E IMPIEGO DI LAVORATORI IRREGOLARI (R15)

- Redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni in materia di selezione e assunzione dei lavoratori stranieri ed a consentire un controllo efficace sui comportamenti e sulle attività della Società e dei suoi subappaltatori
- Nei contratti stipulati con partner commerciali/finanziari devono essere previste clausole che specifichino il richiamo espresso al codice etico aziendale
- Nella selezione dei fornitori è sempre necessario valutare con particolare attenzione l'affidabilità di tali partner ai fini della prevenzione dei reati di cui alla presente parte speciale, anche attraverso indagini ex ante (specie in relazione a particolari indicatori di rischio quali il costo della manodopera del fornitore, l'allocazione degli insediamenti produttivi, ecc.)

REATI DI XENOFOBIA E ISTIGAZIONE AL RAZZISMO (R16)

- Redazione e conservazione della documentazione necessaria a fornire evidenza del rispetto delle prescrizioni in materia di lotta alla xenofobia e all'istigazione al razzismo (evidenze raccolte mediante assunzioni, gestione del personale, rapporto con i fornitori e partner, sponsorizzazioni)

REATI TRIBUTARI (R17)

- Verificare sempre la congruità delle offerte commerciali di acquisto rispetto alle specifiche tecniche
- Verificare sempre la rispondenza dei servizi e/o prodotti forniti/acquistati, rispetto a quanto contrattualmente pattuito
- Non concedere a soggetti terzi sconti, premi, note di credito o la riduzione in qualsiasi altra forma della somma dovuta che non trovino adeguata giustificazione alla luce del rapporto contrattuale con essi costituito e non siano motivati da fattori obiettivi
- Osservare rigorosamente tutte le disposizioni di legge, considerando anche le istruzioni emanate dalle Autorità pubbliche competenti, e le linee guida della Società in materia di predisposizione delle dichiarazioni fiscali e liquidazione e calcolo dei tributi
- Promuovere l'informazione e la formazione interna in tema di fiscalità e garantire la più ampia diffusione e conoscenza alle funzioni aziendali competenti delle suddette linee guida
- Prevedere ed implementare specifiche forme di monitoraggio e controllo delle scadenze relative agli adempimenti di natura fiscale, sia manuali che di sistema
- Privilegiare, nella valutazione delle implicazioni fiscali delle operazioni poste in essere, gli approcci e le logiche di natura prudenziale, nel rispetto rigoroso della normativa e delle procedure aziendali applicabili
- Disciplinare i rapporti con consulenti fiscali e in ogni caso con eventuali terzi coinvolti nei processi sensibili (per autoriciclaggio, in particolare) mediante contratti formalizzati che identifichino in modo puntuale, tra gli altri aspetti, i rispettivi ambiti di attività e responsabilità e che contengano apposita clausola di impegno al rispetto delle previsioni del Modello e del Codice Etico, a pena di risoluzione del contratto
- Disciplinare la gestione del processo fiscale e degli adempimenti ad esso connessi mediante linee guida che consentano di regolare tutte le fasi

## COSA E' VIETATO

E' assolutamente vietato:

- Violare i principi previsti nel Codice Etico
- Violare le regole, norme e prassi operative contenute
  - nelle procedure e, in generale, nella documentazione adottata in attuazione del principi di riferimento previsti nella presente Parte Speciale
  - definite dalle procedure del Sistema di Gestione della Sicurezza della Società
  - dalle procedure del Sistema di Gestione Ambientale della Società
- Violare qualsiasi altra regola contenuta nelle procedure aziendali, nel Codice Etico, nel Modello ed in tutti gli atti adottati in esecuzione dei medesimi, avuto particolare riguardo all'esigenza di prevenire il coinvolgimento di SERENITY S.p.A. in fatti, comportamenti, relazioni o contatti a sfondo terroristico – eversivo e per reati di criminalità organizzata.

- Porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che – considerati individualmente o collettivamente – integrino, direttamente o indirettamente, le fattispecie di reato, anche tentato, rientranti tra quelle richiamate dal D.Lgs. 231/01
- Effettuare elargizioni in denaro a pubblici funzionari italiani o stranieri, sia direttamente da parte di enti italiani o da loro dipendenti, sia tramite persone che agiscono per conto di tali enti sia in Italia che all'estero
- Distribuire omaggi e regali al di fuori di quanto previsto dalla prassi aziendale (vale a dire ogni forma di regalo offerto eccedente le normali pratiche commerciali o di cortesia, o comunque rivolto ad acquisire trattamenti di favore nella conduzione di qualsiasi attività aziendale). In particolare, è vietata qualsiasi regalia a funzionari pubblici italiani ed esteri o a loro familiari (in quei paesi in cui l'elargizione di doni rappresenta una prassi diffusa, è possibile agire in tal senso quando i doni dovranno essere di natura appropriata e di modico valore, ma sempre nel rispetto delle leggi vigenti), che possa influenzare l'indipendenza di giudizio o indurre ad assicurare un qualsiasi vantaggio per l'azienda. Gli omaggi consentiti si caratterizzano sempre per l'esiguità del loro valore o perché volti a promuovere iniziative di carattere benefico o culturale, o la brand image del Gruppo. I regali offerti – salvo quelli di modico valore – devono essere documentati in modo adeguato per consentire le verifiche da parte dell'Organismo di Vigilanza
- Fare o accettare regali, liberalità o pagamenti, specialmente nei rapporti con i Paesi a rischio, che non trovino adeguata giustificazione in un rapporto contrattuale o in un intento benefico adeguatamente documentato ed autorizzato
- Accordare vantaggi di qualsiasi natura (promesse di assunzione, ecc.) in favore di rappresentanti della Pubblica Amministrazione italiana o straniera che possano determinare le stesse conseguenze previste al precedente punto
- Influenzare, nel corso di una qualsiasi trattativa d'affari, richiesta o rapporto con la Pubblica Amministrazione, le decisioni dei funzionari che trattano o prendono decisioni per conto della PA
- Farsi rappresentare nei rapporti con la PA, da consulenti o soggetti terzi che possano creare conflitti di interesse
- Sollecitare od ottenere informazioni riservate che possano compromettere l'integrità o la reputazione di entrambe le parti
- Effettuare prestazioni in favore delle Società di Service, dei Consulenti e dei Partner che non trovino adeguata giustificazione nel contesto del rapporto contrattuale costituito con gli stessi
- Riconoscere compensi in favore delle Società di Service, dei Consulenti, dei Partner e dei Fornitori che non trovino adeguata giustificazione in relazione al tipo di incarico da svolgere ed alle prassi vigenti in ambito locale
- Riconoscere compensi, offrire o promettere vantaggi di qualsiasi natura a dipendenti/ clienti/ fornitori/ partner che non trovino adeguata giustificazione nel contesto del rapporto di lavoro o del rapporto contrattuale costituito con gli stessi.
- Presentare dichiarazioni non veritiere ad organismi pubblici nazionali o comunitari al fine di conseguire erogazioni pubbliche, contributi o finanziamenti agevolati
- Destinare somme ricevute da organismi pubblici nazionali o comunitari a titolo di erogazioni, contributi o finanziamenti per scopi diversi da quelli cui erano destinati
- Tenere comportamenti che abbiano lo scopo o l'effetto di indurre una persona a rilasciare false dichiarazioni davanti all'Autorità giudiziaria
- Rappresentare o trasmettere per l'elaborazione e la rappresentazione in bilanci, relazioni e prospetti o altre comunicazioni sociali, dati falsi, lacunosi o, comunque, non rispondenti alla realtà, sulla situazione economica, patrimoniale e finanziaria della società e delle sue controllate
- Omettere dati ed informazioni imposti dalla legge sulla situazione economica, patrimoniale e finanziaria della società e delle sue controllate

- Restituire conferimenti ai soci o liberare gli stessi dall'obbligo di eseguirli, al di fuori dei casi di legittima riduzione del capitale sociale
- Ripartire utili o acconti su utili non effettivamente conseguiti o destinati per legge a riserva
- Effettuare riduzioni del capitale sociale, fusioni o scissioni, in violazione delle disposizioni di legge a tutela dei creditori, provocando ad essi un danno
- Procedere a formazione o aumento fittizi del capitale sociale, attribuendo azioni per un valore inferiore al loro valore nominale in sede di aumento del capitale sociale
- Diffondere a terzi le credenziali di accesso al programma gestionale nel quale vengono effettuate le registrazioni contabili
- Porre in essere qualsiasi situazione il cui scopo si rivolga o si risolva essenzialmente
  - nella falsificazione delle registrazioni contabili
  - nel deterioramento significativo e misurabile, diretto ed indiretto, di una risorsa naturale o dell'utilità assicurata da quest'ultima
  - nel danneggiamento di informazioni, dati o programmi informatici ovvero di sistemi informatici o telematici
  - nella falsificazione di un documento informatico
  - nel compiere atti di illecita concorrenza, frodi contro l'industria e il commercio ovvero attività finalizzate a turbare la libertà dell'iniziativa economica
  - nel compiere atti di illecita concorrenza, frodi contro l'industria e il commercio ovvero attività finalizzate a turbare la libertà dell'iniziativa economica
- Alterare, contraffare o distruggere documenti contabili
- Sopravvalutare o sottovalutare artificiosamente poste di bilancio allo scopo di fornire un'informazione non veritiera e corretta della situazione economico/ patrimoniale della società
- Omettere o alterare informazioni obbligatorie riguardanti i prospetti di bilancio, la Nota Integrativa, la Relazione sulla Gestione
- Ostacolare le operazioni di controllo da parte del Revisore
- Ostacolare le operazioni di controllo e/o vigilanza dell'OdV riguardanti il corretto rispetto dei principi di redazione/formazione del Bilancio d'esercizio
- Impedire l'attività dell'autorità giudiziaria ovvero comprometterne l'efficacia
- Porre in essere operazioni simulate o diffondere notizie false sulla società
- Dare o promettere denaro o altra utilità agli amministratori, ai dirigenti preposti alla redazione dei documenti contabili societari, ai sindaci, ai liquidatori, nonché alle persone sottoposte alla direzione o vigilanza di uno dei soggetti appena indicati, al fine di trarne vantaggio per la società a danno dell'altra parte
- Porre in essere comportamenti che impediscano materialmente, mediante l'occultamento di documenti o l'uso di altri mezzi fraudolenti, o che comunque ostacolino lo svolgimento dell'attività di controllo e di revisione
- Tenere qualsiasi comportamento che sia di ostacolo all'esercizio delle funzioni di vigilanza anche in sede di ispezione da parte delle Autorità Pubbliche di Vigilanza (espressa opposizione, rifiuti pretestuosi, o anche comportamenti ostruzionistici o di mancata collaborazione, quali ritardi nelle comunicazioni o nella messa a disposizione di documenti).
- Introdurre o spendere in uno qualunque dei siti dove SERENITY ha operatività (sede legale, depositi, altri siti) monete falsificate, anche se ricevute in buona fede
- Porre in atto qualsiasi attività, all'interno dei siti dove SERENITY ha operatività (sede legale, depositi, altri siti), finalizzata all'alterazione/ falsificazione/ contraffazione di monete, valori di bollo o carta filigranata

- Intraprendere o proseguire rapporti o contatti di qualsiasi genere, ivi inclusi il rapporto di agenzia e quello di lavoro subordinato, con soggetti od organizzazioni non preventivamente selezionati o non sottoposti a verifiche successive secondo apposite procedure interne, o che risultino carenti - anche per cause sopravvenute - di alcuno dei requisiti previsti a tali fini. Assume una particolare rilevanza, in proposito, l'eventuale inclusione di tali soggetti od organizzazioni nelle liste dei sospettati di collusione con organizzazioni terroristiche, di volta in volta aggiornate e diramate dalle competenti autorità nazionali o sovranazionali
- Porre in essere comportamenti tali da integrare, anche solo potenzialmente, anche a titolo di concorso o di tentativo, le fattispecie di reato di cui sopra
- Impiegare gli strumenti informatici messi a disposizione dalla Società per procurarsi, disporre, distribuire, divulgare o pubblicizzare materiale pornografico ovvero per distribuire o divulgare notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale
- Organizzare o propagandare iniziative turistiche finalizzate alla fruizione di attività di prostituzione
- Far transitare attraverso canali non ufficiali, e quindi non "tracciabili", flussi finanziari o altre utilità, anche in modo frazionato diretti verso altri Paesi, con particolare attenzione a quelli ad elevato rischio terroristico, ivi inclusi i casi di adesione a iniziative benefiche o di solidarietà, rispetto alle quali s'impone una previa verifica di attendibilità. E' vietato effettuare elargizioni in denaro a individui, società od organizzazioni anche solo sospettate di svolgere attività terroristiche o sovversive dell'ordine pubblico. L'OdV deve in ogni caso essere informato preventivamente in modo circostanziato dell'invio di tali flussi o utilità
- Far transitare attraverso canali non ufficiali e, quindi, non tracciabili, flussi finanziari o altre utilità diretti, anche in modo frazionato, verso soggetti od organizzazioni ad elevato rischio criminale
- Utilizzare Informazioni Privilegiate in funzione della propria posizione all'interno del Gruppo o per il fatto di essere in rapporti d'affari con il Gruppo, per negoziare, direttamente o indirettamente, azioni di una società del Gruppo, di società clienti o concorrenti, o di altre società per trarne un vantaggio personale, così come per favorire soggetti terzi o la società o altre società del Gruppo
- Rivelare a terzi Informazioni Privilegiate relative al Gruppo, se non nei casi in cui tale rivelazione sia richiesta da leggi, da altre disposizioni regolamentari o da specifici accordi contrattuali con cui le controparti si siano impegnate per iscritto a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità
- Partecipare a gruppi di discussione su Internet aventi ad oggetto strumenti finanziari, quotati o non quotati, o valutazioni di quotazioni, e nei quali vi sia uno scambio di informazioni concernenti il Gruppo, le sue società, società concorrenti o società quotate in genere o strumenti finanziari emessi da tali soggetti, a meno che non si tratti di incontri istituzionali per i quali è già stata compiuta una verifica di legittimità da parte delle funzioni competenti o non vi sia scambio di informazioni il cui carattere non privilegiato sia evidente
- Agire di concerto per acquisire una posizione dominante sull'offerta o sulla domanda che abbia l'effetto di fissare, direttamente o indirettamente, i prezzi di acquisto o di vendita o determinare altre condizioni commerciali non corrette
- Diffondere una valutazione su uno strumento finanziario dopo aver precedentemente preso posizione sullo strumento finanziario, beneficiando di conseguenza dell'impatto della valutazione diffusa sul prezzo di detto strumento, senza avere allo stesso tempo comunicato al pubblico l'esistenza di tale conflitto di interesse
- Effettuare operazioni di acquisto o di vendita di uno strumento finanziario senza che si determini alcuna variazione negli interessi o nei diritti o nei rischi di mercato del beneficiario delle operazioni o dei beneficiari che agiscono di concerto o in modo collusivo
- Inserire ordini, specie nei mercati telematici, a prezzi più alti (bassi) di quelli delle proposte presenti dal lato degli acquisti (vendite) al fine di fornire indicazioni fuorvianti dell'esistenza di una domanda (offerta) sullo strumento finanziario a tali prezzi significativamente più elevati (bassi)

- Acquistare o vendere intenzionalmente strumenti finanziari o contratti derivati verso la fine delle negoziazioni in modo da alterare il prezzo finale dello strumento finanziario o del contratto derivato, fatta salva la normale attività di investimento prudenziale di acquisto e vendita di strumenti finanziari o contratti derivati
- Colludere sul mercato secondario dopo un collocamento effettuato nell'ambito di un'offerta al pubblico
- Abusare della propria posizione dominante in modo da distorcere significativamente il prezzo al quale altri operatori sono obbligati, per l'assolvimento dei loro impegni, a consegnare o ricevere o rinviare la consegna dello strumento finanziario o del prodotto sottostante
- Concludere operazioni o impartire ordini in modo tale da evitare che i prezzi di mercato degli strumenti finanziari del Gruppo scendano al di sotto di un certo livello, principalmente per sottrarsi alle conseguenze negative derivanti dal connesso peggioramento del rating degli strumenti finanziari emessi. Questo comportamento deve essere tenuto distinto dalla conclusione di operazioni rientranti nei programmi di acquisto di azioni proprie o nella stabilizzazione degli strumenti finanziari previsti dalla normativa
- Concludere operazioni in un mercato su uno strumento finanziario con la finalità di influenzare impropriamente il prezzo dello stesso strumento finanziario o di altri strumenti finanziari collegati negoziati sullo stesso o su altri mercati
- Diffondere informazioni di mercato false o fuorvianti tramite mezzi di comunicazione, compreso Internet, o tramite qualsiasi altro mezzo
- Prendere una posizione ribassista su uno strumento finanziario ed effettuare un'ulteriore attività di vendita e diffondere fuorvianti informazioni negative sullo strumento finanziario in modo da ridurne il prezzo
- Aprire una posizione su uno strumento finanziario e chiuderla immediatamente dopo che è stata resa nota al pubblico
- Operare creando inusuali concentrazioni di operazioni in concerto con altri soggetti su un particolare strumento finanziario.
- Offrire denaro o altra utilità a qualsivoglia autorità giudiziaria e, più in generale, non relazionarsi con le suddette Autorità senza la preventiva autorizzazione da parte del responsabile
- Avvalersi, nell'espletamento della propria attività ed in maniera diretta o indiretta, della collaborazione di personale clandestino; od omettere di verificare la regolarità del permesso di soggiorno, in sede di assunzione di personale extracomunitario (cfr. parte speciale contro i reati di immigrazione clandestina e impiego di lavoratori irregolari)
- Ricevere denaro contante da soggetti terzi (persone fisiche e/o giuridiche) nell'espletamento della propria attività lavorativa
- Fornire qualsivoglia dato e/o informazione all'esterno, senza il preventivo vaglio e la preventiva autorizzazione da parte dell'unità organizzativa che ha prodotto il dato o gestito l'informazione
- Rappresentare o trasmettere dati falsi, lacunosi o, comunque, non rispondenti alla realtà su:
  - acquisti, vendite o altre operazioni aventi ad oggetto delle partecipazioni societarie
  - acquisti o vendite di prodotti con nomi, marchi o segni distintivi protetti ovvero con caratteristiche di origine, provenienza, qualità o quantità dichiarate
- Acquistare, ricevere o occultare denaro o cose di provenienza illecita o, comunque, intromettersi nel farli acquistare, ricevere o occultare
- Sostituire o trasferire denaro, beni o utilità di provenienza illecita ovvero compiere in relazione ad essi altre operazioni atte ad ostacolare l'identificazione della loro provenienza illecita
- Impiegare in attività economiche e finanziarie denaro, beni o utilità di provenienza illecita

- Assegnare incarichi di fornitura in assenza di autorizzazione alla spesa e dei necessari requisiti di professionalità del Fornitore nonché in assenza della qualità e convenienza del bene o servizio fornito
- Acquistare prodotti e/o servizi non giustificati da concrete esigenze aziendali, motivate e risultanti da evidenze interne quanto a finalità dell'acquisto
- Procedere all'attestazione di regolarità in fase di ricezione di beni/servizi in assenza di un'attenta valutazione di merito e di congruità in relazione al bene/servizio ricevuto e di procedere all'autorizzazione al pagamento di beni/servizi in assenza di una verifica circa la congruità della fornitura/prestazione rispetto ai termini contrattuali
- Pagare agli amministratori emolumenti non deliberati ovvero deliberati, ma in misura sproporzionata all'attività
- Pagare ai parenti degli amministratori per non meglio precisate attività di consulenza
- Pagare compensi agli amministratori a titolo di consulenza
- Pagare consulenze a società che si trovano in paesi black list o off-shore
- Movimentare eccessivamente i conti di cassa senza una descrizione analitica delle operazioni compiute nel mastrino di cassa o nel libro giornale
- Effettuare sponsorizzazioni o donazioni per importi sensibili a Fondazioni o Onlus non meglio individuate ed in violazione con i principi del codice etico
- Effettuare operazioni di significativo ammontare in assenza di motivazioni correlate al proprio business/ attività
- Effettuare operazioni ripetute e di ammontare significativo effettuate in contropartita con società che risultano create di recente e hanno un oggetto sociale generico o incompatibile con il business della società
- Stipulare rapporti contrattuali con vincoli o pegni a favore di terzi che non presentano alcun collegamento con la società
- Acquistare ingenti ammontare di strumenti finanziari a elevata liquidità seguiti dalla richiesta di prestiti garantiti dagli stessi strumenti finanziari
- Effettuare frequenti operazioni di investimento a lungo termine in strumenti finanziari immediatamente seguite dalla richiesta di liquidare la posizione e di trasferire i relativi proventi
- Alterare documenti informatici, pubblici o privati, o aventi efficacia probatoria al fine, ad esempio, di formare, ovvero concorrere a formare con un pubblico ufficiale o incaricato di pubblico servizio - documenti informatici falsi
- Contraffare o alterare - ovvero concorrere a contraffare o alterare con un pubblico ufficiale o incaricato di pubblico servizio - documenti informatici veri, certificati o autorizzazioni amministrative contenute in un documento informatico ovvero le condizioni richieste per la loro validità
- Formare - ovvero concorrere a formare con un pubblico ufficiale o incaricato di pubblico servizio - una copia su documento informatico di un atto pubblico o privato inesistente ovvero una copia diversa dall'originale
- Contraffare - ovvero concorrere a contraffare con un pubblico ufficiale o incaricato di pubblico servizio - un attestato
- Concorrere con un pubblico ufficiale o incaricato di pubblico servizio a formare in un documento informatico una falsa attestazione da parte di quest'ultimo
  - che è un fatto è stato da lui compiuto o avvenuto alla sua presenza
  - che una dichiarazione non resa sia da lui stata ricevuta o che dichiarazioni da lui ricevute siano omesse o alterate

- Concorrere con esercenti la professione sanitaria o forense o altro servizio di pubblica necessità a attestare falsamente sotto forma di documento informatico fatti per i quali il documento stesso è destinato a provare la verità
- Attestare falsamente sotto forma di documento informatico in un atto pubblico o verso un pubblico ufficiale fatti per i quali il documento stesso è destinato a provare la verità
- Formare sotto forma di documento informatico scritture private, in tutto o in parte, false o alterare scritture private vere, utilizzandole o lasciando che altri le utilizzino
- Scrivere o lasciar scrivere su documenti o database informatici dati ed indicazioni falsi soggetti ad ispezione dell'autorità giudiziaria o notificazioni dirette all'autorità giudiziaria con false indicazioni su operazioni industriali, commerciali o professionali
- Scrivere o far scrivere su un documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto privato produttivo di effetti giuridici diversi da quelli previsti, utilizzandolo o lasciando che altri lo utilizzino
- Scrivere o far scrivere ovvero concorrere a scrivere o a far scrivere con un pubblico ufficiale o incaricato di pubblico servizio - su un documento informatico firmato in bianco o con spazi in bianco, posseduto con l'obbligo o il diritto di riempirlo, un atto pubblico diverso da quello cui il pubblico ufficiale o incaricato di pubblico servizio era obbligato o autorizzato
- Distruggere, sopprimere, occultare, in tutto o in parte, una scrittura privata o un atto pubblico veri e disponibili sotto forma di documento informatico
- Utilizzare abusivamente la firma digitale aziendale o, comunque, in violazione delle procedure che ne regolamentano l'utilizzo
- Accedere abusivamente in un sistema informatico o telematico protetto da misure di sicurezza ovvero permanere nel sistema contro la volontà espressa o tacita di chi ha il diritto di escluderlo al fine, ad esempio, di acquisire informazioni mirate allo spionaggio industriale
- Acquisire informazioni facenti capo a concorrenti, potenziali clienti ovvero enti detentori di dati di interesse mirate allo sviluppo di un'offerta commerciale o di una nuova iniziativa
- Alterare dati e informazioni relativi alla Società che sono detenuti da banche o pubbliche amministrazioni
- alterare dati e informazioni che, relativi ad una commessa ultimata o in corso di esecuzione da parte della Società, sono detenuti dal cliente
- Alterare informazioni contenute nei sistemi informatici aziendali allo scopo, ad esempio, di manipolare i dati destinati a confluire nel bilancio della Società
- Acquisire, riprodurre, diffondere, comunicare, consegnare abusivamente codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza o fornire indicazioni o istruzioni idonee allo scopo
- Acquisire, produrre, riprodurre, importare, diffondere, comunicare, consegnare, mettere a disposizione di altri apparecchiature, dispositivi o programmi informatici allo scopo di danneggiare illecitamente un sistema informatico o telematico, i dati o i programmi ivi contenuti o ad esso pertinenti, ovvero di interrompere totalmente o parzialmente o alterare il suo funzionamento
- Intercettare, impedire o interrompere comunicazioni informatiche o telematiche ovvero diffondere al pubblico il contenuto, totale o parziale, di tali comunicazioni mediante un qualsiasi mezzo di informazione al fine, ad esempio, di intercettare fraudolentemente comunicazioni di concorrenti nell'ambito della partecipazione ad una gara d'appalto o di fornitura svolta su base elettronica al fine di falsarne o conoscerne preventivamente l'esito
- Impedire o interrompere comunicazioni di concorrenti allo scopo, ad esempio, di ostacolare l'invio della documentazione d'offerta per la partecipazione ad una gara d'appalto o di altro materiale allo scopo, ad esempio, di determinare un'inadempienza del concorrente nei riguardi del cliente
- Installare apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero comunicazioni intercorrenti tra più sistemi

- Prestare o cedere a terzi apparecchiature informatiche aziendali senza la preventiva autorizzazione del responsabile dei sistemi informatici
- Lasciare incustodito e/o accessibile ad altri il proprio personal Computer ovvero consentire l'utilizzo dello stesso ad altre personale (familiari, amici, etc.)
- Utilizzare password di altri utenti aziendali e l'accesso ad aree protette in nome e per conto di essi, salvo espressa autorizzazione del responsabile dei sistemi informatici ovvero del proprio responsabile
- Divulgare, cedere o condividere con altri le proprie credenziali di accesso ai sistemi informatici della Società, ovvero ai sistemi informatici di clienti, partner o enti terzi
- Ottenere credenziali di accesso ai sistemi informatici della Società, ovvero dei sistemi informatici di clienti, partner o enti terzi, con metodi o procedure differenti da quelle autorizzate allo scopo
- Comunicare a persone non autorizzate, interne o esterne alla Società, i controlli implementati sui sistemi informativi aziendali e le modalità con cui gli stessi sono utilizzati
- Sfruttare eventuali "buchi" nelle misure di sicurezza dei sistemi informatici aziendali, ovvero dei sistemi informatici di clienti, partner o enti terzi, per ottenere l'accesso a risorse o informazioni diverse da quelle per le quali si è autorizzati ad accedere, e ciò anche nel caso in cui l'intrusione non provochi danni a archivi, documenti e programmi informatici
- Modificare la configurazione hardware e/o software delle postazioni di lavoro fisse o mobili senza preventiva autorizzazione del responsabile dei sistemi informatici
- Utilizzare strumenti hardware e/o software che potrebbero essere adoperati abusivamente per compromettere la sicurezza di sistemi informatici o telematici ovvero per intercettare comunicazioni informatiche
- Falsificare, alterare o eliminare il patrimonio informatico aziendale, ovvero il patrimonio informatico di clienti, partner o enti terzi, ivi compresi archivi, documenti o programmi informatici
- Introdurre e/o conservare nei sistemi informatici della Società, a qualsiasi titolo e per qualsiasi ragione,
  - materiale informatico di proprietà di terzi, salvo che lo stesso sia stato acquisito con il loro espresso consenso o da loro trasmesso
  - applicazioni informatiche di dubbia provenienza o che non siano state preventivamente approvate dal responsabile dei sistemi informatici
- Trasferire all'esterno della Società e/o trasmettere documentazione riservata di proprietà della Società o qualsiasi altro file se non per finalità strettamente attinenti allo svolgimento delle proprie mansioni e, comunque, previa autorizzazione del proprio responsabile
- Effettuare copie non specificamente autorizzate su supporto informatico di archivi, documenti e programmi
- Effettuare spamming come pure da ogni azione di risposta allo stesso
- Installare programmi che non siano stati preventivamente autorizzati dal responsabile dei sistemi informatici
- Distruggere, danneggiare, rendere totalmente o parzialmente inservibili sistemi informatici o telematici, ovvero programmi, informazioni o dati altrui al fine, ad esempio, di impedire o danneggiare l'attività di un concorrente
- Distruggere, danneggiare, rendere totalmente o parzialmente inservibili sistemi informatici o telematici, ovvero programmi, informazioni o dati di pubblica utilità al fine, ad esempio, di impedire l'attività di un ente di vigilanza o di controllo ovvero comprometterne l'efficacia
- Impedire l'attività dell'autorità giudiziaria ovvero comprometterne l'efficacia
- Fare o accettare liberalità o pagamenti che non trovino adeguata giustificazione in un rapporto contrattuale o in altro intento legittimo adeguatamente documentato ed autorizzato

- Contraffare, alterare o usare marchi o segni distintivi, modelli, disegni o brevetti, nazionali o esteri, di prodotti industriali con riferimento ai quali, con ordinaria diligenza, si possa conoscere l'esistenza di altrui titoli di proprietà industriale;
- Introdurre nello Stato, detenere per la vendita, vendere o mettere altrimenti in circolazione prodotti industriali con marchi o altri segni distintivi, nazionali o esteri, contraffatti o alterati
- Impedire o ostacolare illegittimamente l'esercizio di un'industria o di un commercio ovvero compiere atti di concorrenza sleale
- Realizzare o consegnare al cliente un prodotto con caratteristiche diverse da quelle dichiarate o pattuite e tali da indurre in inganno il cliente sull'origine, provenienza, qualità, quantità, o altre caratteristiche essenziali, del prodotto
- Progettare/ realizzare, utilizzare, detenere per la vendita, vendere o mettere altrimenti in circolazione prodotti realizzati usurpando titoli di proprietà industriale o in violazione degli stessi potendo conoscerne, con ordinaria diligenza, l'esistenza
- Rivelare a terzi informazioni riguardanti le conoscenze tecniche, tecnologiche e commerciali della Società, se non nei casi in cui tale rivelazione sia richiesta dall'Autorità giudiziaria, da leggi o da altre disposizioni regolamentari o laddove sia espressamente prevista da specifici accordi contrattuali con cui le controparti si siano impegnate a utilizzarle esclusivamente per i fini per i quali dette informazioni sono trasmesse e a mantenerne la confidenzialità
- Tentare o porre in essere azioni o comportamenti riconducibili alla diffusione di opere dell'ingegno protette (L. n. 633/41, art. 171, co. 1 lett. a-bis)) o di opere altrui non destinate alla pubblicità (L. n. 633/41, art. 171, co. 3), alla duplicazione o diffusione di programmi informatici e banche dati (L. n. 633/41, art. 171-bis) ovvero di opere cinematografiche, audiovisive, musicali, letterarie, scientifiche, didattiche, ecc. (L. n. 633/41, art. 171-ter)
- Immettere in un sistema di reti telematiche un'opera dell'ingegno protetta
- Usurpare la paternità di un'opera dell'ingegno ovvero deformare o modificare un'opera qualora ne risulti offesa all'onore o alla reputazione dell'autore
- Duplicare o diffondere programmi informatici in violazione dei diritti d'autore ovvero rimuovere o eludere i dispositivi di protezione applicati a programmi informatici protetti
- Riprodurre o diffondere banche dati in violazione dei diritti del costitutore o dei diritti ed obblighi dell'utente ovvero estrarre o reimpiegare banche dati protette
- Duplicare, riprodurre, trasmettere o diffondere in pubblico opere e parti di opere musicali, cinematografiche o audiovisive
- Riprodurre, trasmettere o diffondere in pubblico opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali;
- Rimuovere o alterare le informazioni elettroniche sul regime dei diritti;
- Detenere attrezzature o prodotti aventi la finalità di eludere le misure di protezione di opere dell'ingegno protette

Qui di seguito viene descritto il processo che ha consentito di pervenire ad una mappa documentata delle potenziali modalità attuative degli illeciti di cui al D.Lgs.231/01 e dei relativi presidi di controllo, al fine della valutazione del rischio potenziale di compimento di "reati rilevanti", della corretta progettazione delle misure preventive e della valutazione del "rischio residuo".

Tale metodologia costituisce inoltre base di riferimento per tutti i successivi aggiornamenti degli schemi di analisi della rischiosità, a seguito di cambiamenti organizzativi e/o di variazioni nell'operatività aziendale.

La metodologia di identificazione e valutazione dei rischi è ampiamente trattata nell'ambito del **Risk Assessment Report**, cui in questa sede si rimanda per le delucidazioni di riferimento.

Il lavoro di ricognizione è stato condotto secondo una metodologia di risk management connessa ai rischi previsti dal Decreto:

a) Obiettivi:
   - Analizzare il profilo di rischio di SERENITY con riferimento ai reati previsti dal Decreto
   - Valutare l'impatto dell'integrazione del Modello di Organizzazione, Gestione e Controllo previsto dal Decreto nella realtà di SERENITY

b) Attività svolte:
   - Analisi del sistema di Governo Societario (attribuzioni di poteri e responsabilità)
   - Identificazione delle attività "sensibili" mediante intervista con i responsabili e le figure operative
   - valutazione delle attività tenendo conto di variabili ricollegabili al rischio ed al livello di controllo che l'azienda implementa a fronte dello stesso. Come prima attività sono stati analizzati i documenti dai quali desumere le informazioni relative alla governance organizzativa, acquisendo la seguente documentazione:
     - statuto
     - poteri e procure
     - disposizioni organizzative, organigramma e mansionari
     - comunicazioni interne
     - manuale e procedure del sistema integrato di gestione
     - documentazione tecnica su sicurezza e ambiente.

c) Predisposizione prospetto di sintesi:
   - Associazione reati – processi, con in evidenza le procedure interessate, i vari process owner e tutti i soggetti coinvolti
   - Identificazione degli ambiti di rischio e le conseguenti attività in cui si estrinseca ciascun processo aziendale. Le attività sono state rilevate con la somministrazione di **questionari** e l'esecuzione di **interviste** mirate rivolte ai vertici e alle altre funzioni della Azienda, sulla base di una preselezione, basata sull'individuazione dei processi prodotta nell'ambito del Sistema di Gestione e sull'analisi dell'Organigramma vigente, del mansionario e dello Statuto, incluse le varie procure. Le interviste hanno permesso di spiegare ai responsabili la *ratio* del D.Lgs. 231/01 e le linee guida seguite nell'elaborazione degli schemi di analisi e di pervenire a schemi semplificati, con l'individuazione delle aree a rischio di reato e dei corrispondenti referenti
   - Identificazione delle procedure e delle misure cautelative di prevenzione del rischio e/o del suo contenimento

L'*output* che ne è seguito, è una mappa di gestione del rischio, che ha costituito la base di lavoro per l'individuazione dei presidi procedurali necessari per prevenire il compimento di attività delittuose.

In base ai rischi rilevati con l'analisi, sono state definite misure cautelative trasformate in procedure, che si ispirano al **principio di segregazione delle funzioni**, in base al quale **i soggetti che intervengono in una fase non possono svolgere alcun ruolo nelle altre fasi del processo decisionale**. La separazione dei compiti risponde all'esigenza di evitare che il processo decisionale, o una parte rilevante di esso, resti nelle mani di un'unica funzione, con il rischio di ingenerare conflitti di interessi e asimmetrie informative capaci di far lievitare il rischio-reato.

Ciascuna operazione deve, infine, rispondere al requisito della **tracciabilità**, sì da risultare **individuabile, verificabile e trasparente**.

# 9 ATTIVITÀ DI VERIFICA E VIGILANZA SVOLTE DALL'ODV

…omissis…

# 10 EFFICACE APPLICAZIONE DEL CODE OF ETHICS E DEL PRESENTE DOCUMENTO NEI CONFRONTI DEI DESTINATARI

L'osservanza del Code of Ethics e del presente documento costituisce parte integrante delle obbligazioni contrattuali dei Dipendenti, anche ai sensi e per gli effetti di cui all'art. 2104 cod. civ. .

La violazione del Code of Ethics e del presente documento può costituire inadempimento contrattuale e/o illecito disciplinare e, se del caso, può comportare il risarcimento dei danni eventualmente derivanti alla Società da tale violazione, in conformità alla vigente normativa ed ai contratti collettivi come di volta in volta applicabili.

I Destinatari hanno l'obbligo di osservare le disposizioni di cui al Code of Ethics ed al presente documento sia nei rapporti tra loro (cd. rapporti interni), sia nei rapporti con i terzi (cd. rapporti esterni). In particolare:

- gli Amministratori, Sindaci e Revisori, nell'ambito delle loro funzioni di amministrazione e di controllo, si ispirano ai principi del Code of Ethics e del presente documento
- i Responsabili funzionali uniformano la propria condotta ai principi previsti nel Code of Ethics e nel presente documento e ne esigono il rispetto da parte dei Dipendenti e dei Collaboratori. A tal fine, la condotta dei Responsabili costituisce modello esemplare. Ai fini del Code of Ethics e del presente documento, ciascun Responsabile è responsabile dei collaboratori sottoposti alla sua direzione, coordinamento o controllo e vigila per prevenire violazioni. In particolare, ciascun Responsabile ha l'obbligo di:
  a) comunicare ai propri collaboratori, in maniera chiara, precisa e completa, gli obblighi da adempiere e specificamente l'obbligo di osservanza delle norme di legge, del Code of Ethics e del presente documento
  b) comunicare ai propri collaboratori in maniera inequivocabile che, oltre a disapprovare eventuali violazioni del Code of Ethics e del presente documento, queste ultime possono costituire inadempimento contrattuale e/o illecito disciplinare, in conformità alla normativa vigente, ed essere quindi sanzionabili
  c) riferire tempestivamente, per iscritto, al proprio superiore o all'OdV le proprie rilevazioni nonché le eventuali notizie a lui riferite dai propri collaboratori in merito a potenziali o attuali violazioni del Code of Ethics e del presente documento da parte di qualsiasi Dipendente o Collaboratore
  d) nell'ambito delle funzioni attribuite, attuare o promuovere l'adozione di misure idonee ad evitare la protrazione di violazioni ed impedire ritorsioni a danno dei propri collaboratori o di qualsiasi altro Dipendente o Collaboratore.

Senza pregiudizio delle funzioni attribuite all'OdV nei confronti dei Destinatari, l'adempimento da parte di ciascun Responsabile delle sue funzioni e degli obblighi ad esse correlati è compiuto in conformità alle disposizioni del Code of Ethics e del presente documento, nonché alle conseguenti raccomandazioni o istruzioni dell'Organismo, ed alle procedure di attuazione e controllo di volta in volta adottate dalla Società. Per quanto necessario, la Società promuove l'applicazione del Code of Ethics e del presente documento ai Destinatari anche mediante inserzione, nei rispettivi contratti con SERENITY, di apposite clausole che stabiliscono l'obbligo di osservare le relative disposizioni.

L'OdV vigila sull'attuazione di quanto precede.

L'OdV vigila inoltre affinché la selezione dei candidati a Dipendenti, Collaboratori ed Esponenti Aziendali sia condotta anche al fine di valutare la congruità delle qualità personali e professionali dei candidati selezionati con le disposizioni del presente documento.

### 10.1 Efficacia del Code of Ethics e del presente documento nei confronti di terzi

Il Destinatario che, nell'esercizio delle sue funzioni, entri in contatto con terzi, dovrà:

- informare, per quanto necessario, il terzo degli obblighi sanciti dal Code of Ethics e dal presente documento
- esigere l'osservanza degli obblighi derivanti dal Code of Ethics e dal presente documento che riguardano direttamente l'attività dello stesso; nel caso del Dipendente o del Collaboratore, riferire al proprio Responsabile, e, nel caso del Responsabile o dell'Amministratore, riferire all'OdV qualsiasi condotta di terzi contraria a tali documenti o comunque idonea ad indurre i Destinatari a commettere violazioni degli stessi.

La Società promuove l'applicazione dei principi fondamentali di cui al Code of Ethics ed al presente documento e, tenuto conto dell'ordinamento giuridico, sociale, economico e culturale di riferimento, di tali norme da parte dei terzi con i quali SERENITY intrattiene rapporti, anche mediante inserzione, nei rispettivi modelli e schemi contrattuali tra essi e SERENITY, di apposite clausole che stabiliscono l'obbligo a carico di tali terzi di osservare, nell'ambito delle proprie attività e della propria organizzazione, le disposizioni del presente documento.

L'OdV vigila sull'attuazione di quanto precede.

## 11 SISTEMA DISCIPLINARE E SANZIONATORIO

La violazione dei principi fissati nel Code of Ethics, nel presente documento e nelle procedure previste dai protocolli interni compromette il rapporto fiduciario tra SERENITY ed i propri amministratori, dipendenti, consulenti, collaboratori a vario titolo, clienti, fornitori, partner commerciali e finanziari.

Tali violazioni saranno dunque perseguite dalla società incisivamente, con tempestività ed immediatezza, attraverso provvedimenti disciplinari adeguati e proporzionati, indipendentemente dall'eventuale rilevanza penale di tali comportamenti e dall'instaurazione di un procedimento penale nei casi in cui costituiscano reato.

Gli effetti delle violazioni del Code of Ethics, del presente documento e dei protocolli interni devono essere tenuti in seria considerazione da tutti coloro che a qualsiasi titolo intrattengono rapporti con SERENITY; a tal fine SERENITY provvede a diffondere il Code of Ethics, il presente documento, le procedure e ad informare sulle sanzioni previste in caso di violazione e sulle modalità e procedure di irrogazione.

L'azienda a tutela della propria immagine e a salvaguardia delle proprie risorse non intratterrà rapporti di alcun tipo con soggetti che non intendano operare nel rigoroso rispetto della normativa vigente, e/o che rifiutino di comportarsi secondo i valori ed i principi previsti dal Code of Ethics e dal presente documento ed attenersi alle procedure e regolamenti previsti dai protocolli annessi.

La predisposizione di un efficace sistema sanzionatorio per la violazione delle prescrizioni contenute nel Modello, è condizione essenziale per garantire l'effettività del Modello stesso.

Al riguardo, infatti, l'articolo 6, comma 2, lettera e) del Decreto prevede che i modelli di organizzazione e gestione devono "introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello".

L'applicazione delle sanzioni disciplinari determinate ai sensi del Decreto prescinde dall'esito di eventuali procedimenti penali, in quanto le regole imposte dal Modello sono assunte dalla Società in piena autonomia, indipendentemente dalla tipologia di illecito che le violazioni del Modello stesso possano determinare.

In particolare, SERENITY si avvale di un sistema disciplinare e sanzionatorio che:

1. è diversamente strutturato a seconda dei soggetti destinatari
2. individua esattamente le sanzioni disciplinari da adottarsi nei confronti dei soggetti destinatari per il caso, da parte di questi ultimi, di violazioni, infrazioni, elusioni, imperfette o parziali applicazioni delle prescrizioni contenute nel Modello, il tutto nel rispetto delle relative disposizioni dei CCNL e delle prescrizioni legislative applicabili
3. prevede un apposito documento di irrogazione delle suddette sanzioni (**Sistema Disciplinare e Sanzionatorio**), individuando il soggetto preposto alla loro irrogazione e in generale a vigilare sulla osservanza, applicazione ed aggiornamento del sistema sanzionatorio stesso
4. introduce idonee modalità di pubblicazione e diffusione.

Di seguito è riportato un estratto del sistema disciplinare e sanzionatorio

## 11.1 L'elaborazione e l'adozione del Sistema Disciplinare e Sanzionatorio.

Ai sensi degli artt. 6 e 7 del Decreto ed in funzione dei requisiti ISO37001, il Modello può ritenersi efficacemente attuato, ai fini dell'esclusione di responsabilità della Società, se prevede un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure ivi indicate.

SERENITY ha, quindi, adottato un Sistema Disciplinare e Sanzionatorio ("Sistema Disciplinare") volto a sanzionare la violazione dei principi, delle norme e delle misure previste nel Modello, nel rispetto delle norme previste dalla contrattazione collettiva nazionale, nonché delle norme di legge o di regolamento vigenti.

Sulla scorta di tale Sistema Disciplinare, sono passibili di sanzione sia le violazioni del Modello (e del sistema ISO37001) commesse dai soggetti posti in posizione "apicale" - in quanto titolari di funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità operativa, ovvero titolari del potere, anche solo di fatto, di gestione o di controllo dell'Ente - sia le violazioni perpetrate dai soggetti sottoposti all'altrui direzione o vigilanza o operanti in nome e/o per conto di SERENITY.

Nel rispetto di quanto previsto anche dalla Linee Guida di Confindustria, l'instaurazione di un procedimento disciplinare, così come l'applicazione delle relative sanzioni, prescindono dall'eventuale instaurazione e/o dall'esito di eventuali procedimenti penali aventi ad oggetto le medesime condotte rilevanti ai fini del Sistema Disciplinare.

## 11.2 La struttura del Sistema Disciplinare

Il Sistema Disciplinare si articola in quattro sezioni:

A. nella prima, sono indicati i soggetti passibili delle sanzioni previste, suddivisi in quattro differenti categorie:
    1. gli Amministratori, il Collegio Sindacale e i Revisori
    2. gli altri soggetti in posizione apicale
    3. i dipendenti/ collaboratori
    4. gli altri soggetti tenuti al rispetto del Modello e dei requisiti ISO37001 (ad es., i fornitori, i consulenti, gli agenti, i partner commerciali, altri soci in affari ecc.).

B. nella seconda, sono indicate le condotte potenzialmente rilevanti, suddivise in quattro differenti categorie, graduate secondo un ordine crescente di gravità
C. nella terza, sono indicate, con riguardo ad ognuna delle condotte rilevanti, le sanzioni astrattamente comminabili per ciascuna categoria di soggetti tenuti al rispetto del Modello e del sistema ISO37001. In ogni caso, l'applicazione delle sanzioni deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata
D. nella quarta, è disciplinato il procedimento di irrogazione ed applicazione della sanzione con riguardo a ciascuna categoria di soggetti destinatari del Sistema Disciplinare.

Le previsioni contenute nel Sistema Disciplinare non precludono la facoltà dei soggetti destinatari di esercitare tutti i diritti, ivi inclusi quelli di contestazione o di opposizione avverso il provvedimento disciplinare ovvero di costituzione di un Collegio Arbitrale, loro riconosciuti da norme di legge o di regolamento, nonché dalla contrattazione collettiva o dai regolamenti aziendali applicabili.

## 11.3 SEZIONE I: I soggetti destinatari

### *11.3.1 Gli amministratori (CdA, Amministratore Delegato), il Collegio Sindacale e i Revisori*

Le norme ed i principi contenuti nel Modello e nel sistema ISO37001 devono essere rispettati, in primo luogo, dai soggetti che rivestono, in seno all'organizzazione SERENITY, una posizione cosiddetta "apicale".
A mente dell'art. 5, I comma, lett. a) del Decreto, rientrano in questa categoria le persone "che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità operativa organizzativa dotata di autonomia finanziaria e funzionale", nonché i soggetti che "esercitano, anche di fatto, la gestione o il controllo" dell'Ente.
In tale contesto, assume rilevanza, in primis, la posizione dei componenti degli organi di amministrazione e controllo di SERENITY.

### *11.3.2 Gli altri soggetti in posizione "apicale"*

Nel novero dei soggetti in cd. "posizione apicale", oltre agli Amministratori e ai Revisori, vanno, inoltre, ricompresi, alla stregua dell'art. 5 sopra richiamato, i Responsabili di Funzione dotati di autonomia finanziaria e funzionale, laddove nominati.
Tali soggetti possono essere legati alla Società sia da un rapporto di lavoro subordinato (di seguito, per brevità, "Dirigenti Apicali"), sia da altri rapporti di natura privatistica (ad es., mandato, agenzia, ecc.).

### *11.3.3 I dipendenti*

L'art. 7, IV comma, lett. b) del Decreto prescrive l'adozione di un idoneo Sistema Disciplinare che sanzioni le eventuali violazioni delle misure previste nel Modello (e nel sistema ISO37001) poste in essere dai soggetti sottoposti alla direzione o alla vigilanza di un soggetto "apicale".
Assume rilevanza, a tale proposito, la posizione di tutti i dipendenti SERENITY legati da un rapporto di lavoro subordinato, indipendentemente dal contratto applicato, dalla qualifica e/o dall'inquadramento aziendale riconosciuti (ad es. quadri, impiegati, lavoratori a tempo determinato, lavoratori con contratto di inserimento, ecc.).

### *11.3.4 Gli altri soggetti tenuti al rispetto del Modello*

Il presente Sistema Disciplinare ha, inoltre, la funzione di sanzionare le violazioni del Modello e del sistema ISO37001 commesse da soggetti anche diversi da quelli sopra indicati.
Si tratta, in particolare, di tutti i soggetti (di seguito, per brevità, collettivamente denominati "Terzi Destinatari") che sono comunque tenuti al rispetto del Modello e del sistema ISO37001 in virtù della funzione svolta in relazione alla struttura societaria ed organizzativa, ad esempio in quanto funzionalmente soggetti alla direzione o vigilanza di un soggetto "apicale", ovvero in quanto operanti, direttamente o indirettamente, per SERENITY.
Nell'ambito di tale categoria, possono farsi rientrare i seguenti soggetti:

- tutti coloro che intrattengono con SERENITY un rapporto di lavoro di natura non subordinata (ad es., i collaboratori a progetto)
- i procuratori e tutti coloro che agiscono in nome e/o per conto dell'azienda
- i fornitori ed i partner, inclusi i consulenti a qualsiasi titolo
- i collaboratori a qualsiasi titolo
- i soci in affari.

## 11.4 SEZIONE II: Le condotte rilevanti

Ai fini del presente Sistema Disciplinare, e nel rispetto delle previsioni di cui alla contrattazione collettiva, laddove applicabili, costituiscono condotte oggetto di sanzione le azioni o i comportamenti posti in essere in violazione del Modello e del sistema ISO37001.
In considerazione dell'obbligo gravante, in riferimento al Codice Etico, su ciascun Destinatario di ottemperare alle indicazioni e/o alle prescrizioni provenienti dall'Organismo di Vigilanza e da FDC di SERENITY, costituiscono violazioni del Modello e del sistema ISO37001 anche le condotte, ivi incluse quelle omissive, poste in essere in violazione delle indicazioni e/o delle prescrizioni dell'OdV/FDC.

Nel rispetto del principio costituzionale di legalità, nonché di quello di proporzionalità della sanzione, tenuto conto di tutti gli elementi e/o delle circostanze ad essa inerenti, si ritiene opportuno definire un elenco di possibili violazioni, graduate secondo un ordine crescente di gravità:

**G1.** mancato rispetto del Modello e del sistema ISO37001, qualora si tratti di violazioni connesse, in qualsiasi modo, alle aree indicate quali "strumentali" o "di supporto", e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4

**G2.** mancato rispetto del Modello e del sistema ISO37001, qualora si tratti di violazioni connesse, in qualsiasi modo, alle aree "a rischio reato" o alle attività "sensibili" indicate nel Modello stesso e nel sistema ISO37001, e sempre che non ricorra una delle condizioni previste nei successivi nn. 3 e 4

**G3.** mancato rispetto del Modello e del sistema ISO37001, qualora si tratti di violazione idonea ad integrare uno dei reati previsti nel Decreto (contributo parziale) e/o reati di natura corruttiva

**G4.** mancato rispetto del Modello e del sistema ISO37001, qualora si tratti di violazione finalizzata alla commissione di uno dei reati previsti dal Decreto e/o reati di natura corruttiva, o comunque sussista il pericolo che sia contestata la responsabilità della Società ai sensi del Decreto.

## 11.5 SEZIONE III: Le sanzioni

### *11.5.1 Tipologia di sanzioni e criteri di commisurazione*

Nella presente sezione sono indicate le sanzioni irrogabili a fronte dell'accertamento di una delle violazioni di cui alla Sezione II.
Le sanzioni sono applicate nel rispetto delle previsioni contenute nella Sezione IV, nonché delle norme rinvenibili nella contrattazione collettiva, laddove applicabile.
*In ogni caso, l'individuazione e l'irrogazione delle sanzioni deve tener conto dei principi di proporzionalità e di adeguatezza rispetto alla violazione contestata.*

A tale proposito, avranno rilievo, in via generale, i seguenti elementi e criteri di commisurazione:

- la tipologia dell'illecito compiuto
- le circostanze nel cui ambito si è sviluppata la condotta illecita
- le modalità di commissione della condotta, con particolare attenzione all'intenzionalità del comportamento o al grado di negligenza, imprudenza o imperizia con riguardo anche alla prevedibilità dell'evento
- il comportamento complessivo del lavoratore con particolare riguardo alla sussistenza o meno di precedenti disciplinari del medesimo, nei limiti consentiti dalla legge
- le mansioni del lavoratore
- la posizione funzionale della persona coinvolta nei fatti costituenti la mancanza
- le altre particolari circostanze che possono accompagnare la violazione disciplinare.

Ai fini dell'eventuale aggravamento della sanzione, sono inoltre considerati i seguenti elementi:

- la gravità della condotta
- l'intensità del dolo e del grado della colpa
- l'eventuale commissione di più violazioni nell'ambito della medesima condotta, nel qual caso l'aggravamento sarà operato rispetto alla sanzione prevista per la violazione più grave
- l'eventuale concorso di più soggetti nella commissione della violazione
- l'eventuale recidività del suo autore
- il comportamento tenuto dall'autore della violazione precedentemente e successivamente alla realizzazione della stessa
- la circostanza che la violazione abbia provocato un grave danno alla società ovvero l'abbia esposta ad un procedimento per responsabilità amministrativa da reato, ai sensi del D.Lgs. 231/01
- la circostanza che la violazione abbia esposto la società ad una non conformità grave ai sensi della ISO37001
- le condizioni economiche dell'autore della violazione

Nessuna sanzione può comunque essere irrogata senza aver prima sentito l'interessato, avergli contestato con precisione, e in forma scritta, l'addebito, ed avergli concesso un congruo termine entro il quale esporre per iscritto le proprie ragioni.
L'applicazione delle sanzioni di seguito indicate non pregiudica in ogni caso il diritto della Società di agire nei confronti del soggetto responsabile al fine di ottenere il risarcimento di tutti i danni patiti a causa o in conseguenza della condotta accertata.

#### *11.5.2 Le sanzioni nei confronti degli Amministratori, del Collegio Sindacale e dei Revisori*

…omissis….

#### *11.5.3 Le sanzioni nei confronti dei Dirigenti Apicali e degli Altri Soggetti Apicali*

…omissis….

#### *11.5.4 Le sanzioni nei confronti dei Dipendenti*

…omissis….

#### *11.5.5 Le sanzioni nei confronti dei Terzi Destinatari*

Qualora sia accertata la commissione di una delle violazioni indicate nella Sezione II da parte di un Terzo Destinatario, saranno applicate le seguenti sanzioni:

| **Gravità della violazione** | **Sanzione** |
|---|---|
| G1 | diffida ovvero quella della penale convenzionale ovvero quella della risoluzione, a seconda della gravità della violazione |
| G2 | diffida ovvero quella della penale convenzionale ovvero quella della risoluzione, a seconda della gravità della violazione |
| G3 | penale convenzionale (10% del corrispettivo pattuito o maturato (in relazione alla forma contrattuale in essere) ovvero quella della risoluzione |
| G4 | risoluzione |

Nell'ambito dei rapporti con i Terzi Destinatari, la Società inserisce, nelle lettere di incarico e/o negli accordi negoziali relativi, apposite clausole volte a prevedere, in caso di violazione del Modello e del sistema ISO37001, l'applicazione delle misure sopra indicate.

### 11.6 SEZIONE IV: Il procedimento di irrogazione delle sanzioni

Nella presente sezione sono indicate le procedure da seguire nell'ambito della fase di irrogazione delle sanzioni conseguenti alla eventuale commissione delle violazioni previste nella Sezione II.
In particolare, si ritiene opportuno delineare il procedimento di irrogazione delle sanzioni con riguardo a ciascuna categoria di soggetti destinatari, indicando, per ognuna:

- la fase della contestazione della violazione all'interessato
- la fase di determinazione e di successiva irrogazione della sanzione.

Il procedimento di irrogazione ha, in ogni caso, inizio a seguito della ricezione, da parte degli organi aziendali di volta in volta competenti e di seguito indicati, della comunicazione con cui l'OdV/FDC segnala l'avvenuta violazione del Modello.

Più precisamente, in tutti i casi in cui riceva una segnalazione (anche anonima) ovvero acquisisca, nel corso della propria attività di vigilanza e di verifica, gli elementi idonei a configurare il pericolo di una violazione del Modello e del sistema ISO37001, l'OdV/FDC ha l'obbligo di attivarsi al fine di espletare gli accertamenti ed i controlli rientranti nell'ambito della propria attività.
Esaurita l'attività di verifica e di controllo, l'OdV/FDC valuta, sulla base degli elementi in proprio possesso, se si è effettivamente verificata una violazione del Modello e del sistema ISO37001. In caso positivo, segnala la violazione agli organi aziendali competenti; in caso negativo, trasmette la segnalazione all'Amministratore Delegato e al Responsabile Modello Organizzativo ai fini della valutazione della eventuale rilevanza della condotta rispetto alle altre leggi o regolamenti applicabili.

L'OdV/FDC inoltre trasmette al CdA una **relazione** contenente:

- la descrizione della condotta constatata
- l'indicazione delle previsioni del Modello e del sistema ISO37001che risultano essere state violate
- gli estremi del soggetto responsabile della violazione
- gli eventuali documenti comprovanti la violazione e/o gli altri elementi di riscontro
- una propria proposta in merito alla sanzione opportuna rispetto al caso concreto.

Entro **dieci giorni** dall'acquisizione della relazione dell'OdV/FDC, il CdA convoca il membro indicato dall'OdV/FDC per un incontro, da tenersi entro e **non oltre trenta giorni** dalla ricezione della relazione stessa.

La convocazione deve:

- essere effettuata per iscritto
- contenere l'indicazione della condotta contestata e delle previsioni del Modello e del sistema ISO37001 oggetto di violazione
- comunicare all'interessato la data dell'incontro, con l'avviso della facoltà di formulare eventuali rilievi e/o deduzioni, sia scritte e sia verbali.

La convocazione deve essere sottoscritta dall'Amministratore Delegato o da almeno due membri del CdA.
In occasione dell'adunanza del CdA, a cui è invitato a partecipare anche l'OdV/FDC, vengono disposti l'audizione dell'interessato, l'acquisizione delle eventuali deduzioni da quest'ultimo formulate e l'espletamento degli eventuali ulteriori accertamenti ritenuti opportuni.
Il CdA, sulla scorta degli elementi acquisiti, determina la sanzione ritenuta applicabile, motivando l'eventuale dissenso rispetto alla proposta formulata dall'OdV/FDC.
Qualora la sanzione ritenuta applicabile consista nella decurtazione degli emolumenti o nella revoca dall'incarico, il CdA si attiva per le relative deliberazioni.

La delibera del CdA viene comunicata per iscritto all'interessato nonché all'OdV/FDC, per le opportune verifiche.

Ferma restando la facoltà di adire l'autorità giudiziaria, il dipendente può promuovere, nei venti giorni successivi dalla ricezione del provvedimento disciplinare, la costituzione di un collegio di conciliazione ed arbitrato, secondo quanto previsto dalla contrattazione collettiva applicabile al caso concreto. In caso di nomina del Collegio, la sanzione disciplinare resta sospesa fino alla pronuncia di tale organo.

FINE DEL DOCUMENTO