confidisystema!

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO ex D.Lgs. 231/01

Versione del documento

Versione	*Data*	*Descrizione*
1	Aprile 2014	Stesura del documento
2	Luglio 2018	Aggiornamento
3	15 Dicembre 2022	Aggiornamento

SOMMARIO

PARTE GENERALE

IL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

1.1 Il regime di responsabilità amministrativa-penale a carico di persone giuridiche, società ed associazioni anche prive di personalità giuridica.

Con l'emanazione del D. Lgs. 8 giugno 2001, n. 231, il Legislatore ha parzialmente attuato la Legge delega n. 300/2000, che, a sua volta, ha recepito normative sopranazionali, ossia la Convenzione del 26 maggio 1997, relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle Comunità Europee o degli Stati membri dell'Unione Europea, e la Convenzione OCSE del 17 dicembre 1997, sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali.

Detto Decreto (come integrato dal D.M. n. 201 del 2003 e da successivi interventi legislativi) ha introdotto per la prima volta nel nostro ordinamento la responsabilità di persone giuridiche, società ed associazioni, anche prive di personalità giuridica (di seguito, per brevità, "enti" o "ente"), per attività illecita derivante dalla commissione di alcuni reati, posti in essere a vantaggio e/o nell'interesse dell'ente, da parte di:

- persone fisiche che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente (i cd soggetti apicali) 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 degli stessi;
- persone sottoposte (i cd soggetti sottoposti) alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a);
- soggetti esterni che, operando in nome e/o per conto dell'ente, compiono atti nei confronti dell'esterno.

Ciò significa che, in caso di commissione di uno o più reati espressamente previsti dalla legge ad opera di un soggetto apicale, ovvero di un sottoposto, o di un soggetto esterno all'ente, si aggiunge, alla responsabilità penale dell'autore materiale del reato, la responsabilità amministrativa dell'ente, se il reato è stato commesso nel suo interesse o la Società ne ha comunque tratto un vantaggio.

L'ente è chiamato a rispondere con il proprio patrimonio e la sua responsabilità è autonoma rispetto a quella dell'autore del reato cui si aggiunge anche quando l'autore del reato non è stato individuato o non è imputabile oppure nel caso in cui il reato si estingua per una causa diversa dall'amnistia.

Ai sensi dell'art. 5, comma 2, del Decreto, "l'ente non risponde se le persone sopra indicate hanno agito nell'interesse esclusivo proprio o di terzi".

Ai fini dell'affermazione della responsabilità dell'ente, oltre all'esistenza dei richiamati requisiti che consentono di collegare oggettivamente il reato all'ente, il legislatore impone l'accertamento della colpevolezza dell'ente. Tale condizione si identifica con una colpa da organizzazione, intesa come violazione di adeguate regole di diligenza autoimposte dall'ente medesimo e volte a prevenire lo specifico rischio da reato.

Ai sensi dell'art. 6 del Decreto, la responsabilità amministrativa è esclusa pertanto se l'ente coinvolto dimostra, prima della commissione del reato, di aver adottato ed efficacemente attuato, fra l'altro, Modelli di organizzazione, gestione e controllo idonei a prevenire la realizzazione dei reati previsti dal Decreto sia che il reato sia stato commesso da un soggetto apicale sia che sia stato commesso da un soggetto sottoposto.

1.2 I soggetti destinatari

Ai sensi dell'art. 1, comma 2, del Decreto, la normativa in tema di responsabilità amministrativa degli enti si applica a:
Enti dotati di personalità giuridica, quali, a titolo esemplificativo, S.p.A., S.r.l., S.a.p.A, Cooperative, Associazioni riconosciute, Fondazioni, altri enti privati e pubblici economici;

- Società e associazioni anche prive di personalità giuridica, quali, a titolo esemplificativo, S.n.c. e S.a.s. anche irregolari, Associazioni non riconosciute.
- Restano, invece, esclusi dalla soggezione alla normativa in esame:
- le imprese individuali;
- lo Stato;
- le Regioni;
- le Province;
- i Comuni;
- altri enti pubblici non economici;
- partiti politici;
- sindacati.

1.3 Le fattispecie di reato (i c.d. "reati presupposto")

L'insorgenza della responsabilità in capo all'ente non è conseguente alla commissione di qualsiasi reato, bensì di quelli esclusivamente previsti dalla legge.

I reati da cui può conseguire la responsabilità amministrativa per l'ente sono espressamente indicati nel D.Lgs. 231/2001, nonché in altri provvedimenti di legge che al D.Lgs. 231/2001 fanno rinvio, sono:

- i reati contro la Pubblica Amministrazione o l'Unione europea (art. 25) e contro il patrimonio della Pubblica Amministrazione o dell'Unione Europea (art. 24);
- i delitti informatici, di trattamento illecito di dati, nonché i reati commessi con violazione delle prescrizioni in materia di cyber security (art. 24 bis);
- i delitti di criminalità organizzata (art. 24 ter); i reati in materia di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25 bis);
- i delitti contro l'industria e il commercio (art. 25 bis 1);
- i reati societari (art. 25 ter);
- i reati con finalità di terrorismo o di eversione dall'ordine democratico (art. 25 quater);
- i reati commessi nell'effettuazione di pratiche di mutilazione degli organi genitali femminili (art. 25 quater.1);
- i reati contro la personalità individuale (art. 25 quinquies) ed i reati di abuso di informazioni privilegiate e di manipolazione del mercato (art. 25 sexies);
- una serie di reati (dall'associazione a delinquere, al traffico di stupefacenti, a talune fattispecie di ostacolo alla giustizia) a condizione che siano commessi da organizzazioni criminali che operano a livello internazionale (cd. reati transnazionali);
- i reati di omicidio colposo e lesioni colpose gravissime e gravi commessi con violazione delle norme sulla sicurezza del lavoro (art. 25 septies);
- i reati di ricettazione, riciclaggio e di impiego di denaro, beni o utilità di provenienza illecita nonché di autoriciclaggio (art. 25 octies);
- i delitti in materia di strumenti di pagamento diversi dai contanti (art. 25-octies.1);
- i reati in materia di violazione del diritto d'autore (art. 25 novies), induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 25 decies);

- i reati ambientali (art. 25 undecies), l'inosservanza delle sanzioni interdittive (art. 23);
- il reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare (art. 25 duodecies);
- i reati di razzismo e xenofobia (art. 25-terdecies);
- i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25- quaterdecies);
- i reati tributari (art. 25 – quinquiesdecies);
- il contrabbando (art. 25-sexiesdecies);
- i delitti contro il patrimonio culturale (art. 25-septiesdecies).

Più in particolare, il Decreto 231, nel suo testo originario, prevedeva i soli reati contemplati nelle norme di cui agli artt. 24 e 25: per effetto di provvedimenti normativi successivi la casistica dei reati si è tuttavia notevolmente ampliata.

In particolare, gli articoli 24 e 25 del Decreto contemplano i reati presupposto contro la Pubblica Amministrazione o l'Unione Europea e contro il patrimonio della Pubblica Amministrazione o dell'Unione Europea:

- indebita percezione di contributi, finanziamenti o altre erogazioni da parte dello Stato o di altro ente pubblico (art. 316 ter c.p.);
- malversazione a danno dello Stato (art. 316-bis c.p.);
- truffa in danno dello Stato o di altro ente pubblico o della Comunità europea (art. 640, comma 2, n. 1, c.p.);
- truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640 bis c.p.);
- frode informatica in danno dello Stato o di altro ente pubblico (art. 640 ter c.p.);
- corruzione (artt. 318, 319, 320, 321 e 322 bis c.p.);
- istigazione alla corruzione (art. 322 c.p.);
- corruzione in atti giudiziari (art. 319 ter c.p.);concussione (art. 317 c.p.);
- induzione indebita a dare o promettere utilità (art. 319 quater c.p.);
- traffico di influenze illecite (art. 346 bis c.p.).

Successivamente, l'art. 3 del Decreto Legislativo 11 aprile 2002 n. 61, in vigore dal 16 aprile 2002, nell'ambito della riforma del diritto societario ha introdotto il nuovo art. 25-ter del Decreto 231, poi modificato dalla Legge 28 Dicembre 2005, n. 262, estendendo il regime di responsabilità amministrativa degli enti anche ai c.d. reati societari; più precisamente la responsabilità è stata estesa ai reati di:

- false comunicazioni sociali;
- false comunicazioni sociali in danno dei soci o dei creditori;
- falsità nelle relazioni o nelle comunicazioni della società di revisione;
- impedito controllo;
- indebita restituzione dei conferimenti;
- illegale ripartizione degli utili e delle riserve;
- illecite operazioni sulle azioni o quote sociali o della società controllante;
- operazioni in pregiudizio dei creditori;
- formazione fittizia del capitale;
- indebita ripartizione dei beni sociali da parte dei liquidatori;
- illecita influenza sull'assemblea;
- aggiotaggio;
- ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza;
- omessa comunicazione del conflitto di interessi (introdotto dalla Legge n. 262/2005).

L'art. 25 quater, inserito nel corpus originario del Decreto 231 dall'art. 3 della Legge 14 gennaio 2003, n. 7 (Ratifica della Convenzione internazionale contro il finanziamento del terrorismo), ha esteso la responsabilità amministrativa degli enti ai delitti con finalità di terrorismo e di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali e ai delitti violanti le prescrizioni contenute nella Convenzione summenzionata. Vengono elencati a titolo esemplificativo, ancorché non esaustivo:

- associazioni sovversive (art. 270 c.p.)
- associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico (art. 270-bis c.p.)
- circostanze aggravanti e attenuanti (art. 270-bis.1 c.p.)
- promozione, costituzione, organizzazione o direzione di associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico;
- assistenza agli associati (art. 270-ter c.p.);
- organizzazione di trasferimento per finalità di terrorismo (art. 270-quater.1)
- finanziamento di condotte con finalità di terrorismo (L. n. 153/2016, art. 270-quinquies.1 c.p.)
- sottrazione di beni o denaro sottoposti a sequestro (art. 270-quinquies.2 c.p.)
- condotte con finalità di terrorismo (art. 270-sexies c.p.)
- attentato per finalità terroristiche o di eversione (art. 280 c.p.);
- atto di terrorismo con ordigni micidiali o esplosivi (art. 280-bis c.p.)
- atti di terrorismo nucleare (art. 280-ter c.p.)

L'art. 25 quater.1, inserito nel corpus originario del Decreto 231 dall'art. 3 della Legge 9 gennaio 2006, n. 7 (Disposizioni concernenti la prevenzione ed il divieto delle pratiche di mutilazione genitale femminile), ha esteso la responsabilità amministrativa degli enti al delitto di pratiche di mutilazione degli organi genitali femminili di cui all'art. 583-bis c.p..

L'art. 25 quinquies, inserito nel corpus originario del Decreto 231 dall'art. 5 della Legge 228 dell'11 agosto 2003 e modificato dalla Legge 6 febbraio 2006, n. 38 (Misure contro la tratta di persone), ha ulteriormente esteso la responsabilità amministrativa degli enti ai delitti contro la personalità individuale, quali:

- riduzione in schiavitù;
- tratta e commercio di schiavi;
- alienazione e acquisto di schiavi;
- prostituzione minorile;
- pornografia minorile;
- detenzione di materiale pornografico minorile;
- iniziative turistiche volte allo sfruttamento della prostituzione minorile.

L'art. 25 sexies, inserito nel corpus originario del Decreto 231 dall'articolo 9, comma 3 della Legge 18 aprile 2005 n. 62 (Recepimento della direttiva 2003/6/CE del Parlamento europeo e del Consiglio, del 28 gennaio 2003, relativa all'abuso di informazioni privilegiate e alla manipolazione del mercato - abusi di mercato - e delle direttive della Commissione di attuazione 2003/124/CE, 2003/125/CE e 2004/72/CE) ha ulteriormente esteso la responsabilità amministrativa degli enti ai delitti di abusi di mercato:

- abuso di informazioni privilegiate;
- manipolazione del mercato.

La medesima Legge n. 62 del 2005 ha previsto, inoltre, all'art. 187-quinquies Testo unico della finanza, una nuova forma di responsabilità dell'Ente conseguente alla commissione nel suo interesse o vantaggio (non di reati ma) degli illeciti amministrativi di:

- abuso di informazioni privilegiate (art. 184 Testo unico della finanza);
- manipolazione del mercato (art. 185 Testo unico della finanza);
- responsabilità dell'ente (art. 187-quinquies Testo unico della finanza).

L'art. 10 della Legge 16 marzo 2006, n. 146 - non espressamente richiamata dal Decreto 231 - come successivamente modificata, ha previsto la responsabilità amministrativa degli Enti in relazione ad una serie di reati a carattere "transnazionale" ai sensi dell'art. 3 della predetta Legge (associazione per delinquere, associazione di tipo mafioso, associazione finalizzata al traffico di sostanze stupefacenti, associazione finalizzata al contrabbando di tabacchi lavorati esteri, induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria, favoreggiamento personale, procurato ingresso illegale nel territorio dello Stato italiano o di altro Stato del quale la persona non sia cittadina e favoreggiamento della permanenza illegale).

Si considera reato transnazionale il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato, nonché: a) sia commesso in più di uno Stato; b) ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; c) ovvero sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; d) ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.

Inoltre, la Legge 3 agosto 2007 n.123 ha introdotto nel Decreto 231 l'art. 25 septies, successivamente riformulato dall'art. 300 del D.Lgs. 9 Aprile 2008, n. 81; il suddetto art. 25 septies stabilisce un'ulteriore estensione della responsabilità amministrativa degli Enti in relazione ai delitti di:

- omicidio colposo commesso con violazione dell'articolo 55, comma 2, del decreto legislativo attuativo della delega di cui alla legge 3 agosto 2007, n. 123, in materia di salute e sicurezza sul lavoro;
- omicidio colposo e lesioni colpose gravi e gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

Il decreto legislativo n. 231 del 21 novembre 2007, pubblicato nel supplemento ordinario n. 268 della Gazzetta Ufficiale n. 290 del 14 Dicembre 2007, ha recepito la direttiva 2005/60/CE del Parlamento Europeo e del Consiglio del 26.10.2005, concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo (c.d. Terza direttiva Antiriciclaggio).

Tale decreto legislativo estende l'ambito di applicazione del D.Lgs. 231/2001, introducendovi l'art. 25 octies volto a sanzionare i delitti di:

- ricettazione (art. 648 del Codice Penale);
- riciclaggio (art. 648 bis del Codice Penale);
- impiego di denaro, beni o utilità di provenienza illecita (art. 648 ter del Codice Penale);
- autoriciclaggio (art. 648-ter.1 c.p.).

Nel Supplemento Ordinario n. 28 alla Gazzetta Ufficiale n. 140 del 19 giugno 2017 è stato pubblicato il decreto legislativo 25 maggio 2017, n. 90 (il "Decreto"), che modifica i decreti legislativi 21 novembre 2007 n. 231 (il "Decreto 231") e 22 giugno 2007, n. 109 allo scopo di recepire la Direttiva (UE) 2015/849 ("IV Direttiva AML") in materia di «prevenzione dell'uso del sistema finanziario a fini di riciclaggio o finanziamento del terrorismo» e dare attuazione del Regolamento (UE) 2015/847, concernente «i dati informativi che accompagnano i trasferimenti di fondi».

Il recepimento della IV Direttiva AML ha comportato l'introduzione di rilevanti modifiche all'impianto normativo del Decreto 231, che imporranno ai relativi destinatari l'avvio di un articolato assessment delle policy e procedure interne adottate, onde verificarne per tempo la perdurante adeguatezza alla luce 'delle novità introdotte dal Decreto e dalla concreta operatività.

Tra le novità di maggior rilievo, sicuramente degna di nota appare anzitutto l'inclusione, tra i destinatari degli obblighi antiriciclaggio, degli intermediari bancari e finanziari europei operanti in Italia in regime di libera

prestazione di servizi su base cross-border, nonché dei consulenti finanziari e delle società di consulenza finanziaria di cui, rispettivamente, agli articoli 18-bis e ter del Testo Unico della Finanza.

La Direttiva UE 2018/843 (i.e. V Direttiva Antiriciclaggio), pubblicata sulla Gazzetta Ufficiale dell'UE in data 19 giugno 2018, ha poi apportato alcune modifiche alla precedente Direttiva UE 2015/849 (i.e. IV Direttiva Antiriciclaggio).

L'adozione della V Direttiva Antiriciclaggio affonda le proprie radici nella necessità di potenziare, attraverso l'imposizione di maggiori obblighi di trasparenza, la lotta contro il riciclaggio di denaro e il finanziamento del terrorismo in tutta l'Unione europea.

Tale necessità di un nuovo quadro normativo più ampio deriva dalle recenti vicende che hanno coinvolgo la comunità internazionale (terrorismo internazionale, scandalo Panama Papers, etc.).

In tale ottica, il nuovo corpus normativo dovrebbe rispondere alla necessità di (i) rafforzare le attività di individuazione e prevenzione di movimenti di fondi e altri beni, (ii) implementare la tracciabilità dei mezzi finanziari quale strumento di contrasto al terrorismo e (iii) contrastare la capacità di raccolta di fondi finalizzati a finanziare attività illecite.

Le modifiche apportate alla V Direttiva Antiriciclaggio riguardano in primo luogo l'ampliamento dell'ambito soggettivo ed oggettivo di applicazione delle disposizioni in materia di individuazione delle operazioni sospette sui fenomeni di riciclaggio e finanziamento del terrorismo.

In particolare, tale ampliamento si riscontra relativamente alle seguenti operazioni e attività:

- commercio di opere d'arte (anche quando effettuate da galleristi, gestori di case d'asta e antiquari);
- conservazione o commercio di opere d'arte effettuate da porti franchi;
- impegno a fornire aiuto materiale, assistenza o consulenza in materia fiscale quale attività imprenditoriale o professionale principale;
- agenzia immobiliare; e
- operazioni in valuta virtuale e servizi di portafoglio digitale.

Il decreto legislativo di attuazione della V Direttiva Antiriciclaggio (Decreto 125/2019), recentemente approvato dal Consiglio dei Ministri, ha esteso gli obblighi antiriciclaggio anche alle attività sottostanti alle operazioni di cartolarizzazione di crediti disciplinate dalla Legge del 30 aprile 1999, n. 130. In particolare, è previsto l'inserimento del comma 2-bis all'art. 3 del D.lgs. 231/2007 il quale stabilisce che gli intermediari bancari e finanziari «incaricati della riscossione dei crediti ceduti, dei servizi di cassa e di pagamento e delle verifiche di conformità», devono provvedere all'adempimento degli obblighi antiriciclaggio «anche nei confronti dei debitori ceduti alle società di cartolarizzazione dei crediti nonché dei sottoscrittori dei titoli emessi dalle medesime società».

Tale presidio è evidentemente finalizzato a sottoporre agli obblighi antiriciclaggio tutti quei soggetti che, nell'ambito di complesse operazioni di cartolarizzazione, intervengono, anche come semplici veicoli, nei flussi di denaro.

La V Direttiva Antiriciclaggio modifica l'art. 31 della Direttiva UE 2015/849 e introduce alcune novità con riguardo all'individuazione del titolare effettivo per i trust e per altri tipi di istituti giuridici (tra cui le fiduciarie) che abbiano assetto o funzioni affini a quelli dei trust.

Più precisamente, con riguardo alle informazioni sulla titolarità effettiva da comunicare al Registro centrale dei titolari effettivi istituito dallo Stato membro in cui è stabilito o risiede il trustee (o la persona che ricopre una posizione equivalente), si prevede che siano tenuti all'obbligo comunicativo i trust espressi e gli istituti giuridici affini, sostituendo la precedente previsione che riguardava solo i trust produttivi di effetti giuridici rilevanti a

fini fiscali secondo quanto disposto dall'art. 73 del TUIR (trust produttivi di effetti giuridici rilevanti a fini fiscali, per i quali è espressamente previsto l'obbligo di iscrizione in apposita sezione speciale del Registro delle imprese).

In seguito alle modifiche introdotte dalla V Direttiva Antiriciclaggio, l'obbligo comunicativo dovrà riguardare tutte le tipologie di trust nonché i c.d. "istituti giuridici affini"; con riguardo a questi ultimi, al fine di garantire la certezza del diritto, è inoltre previsto che gli Stati membri definiscano le caratteristiche in base alle quali determinare se un istituto giuridico abbia assetto o funzioni affini a quelle dei trust.

La V Direttiva ha introdotto specifiche misure, estendendo gli obblighi antiriciclaggio a due tipologie di soggetti individuati tra i prestatori di servizi la cui attività consiste nella fornitura di servizi di cambio tra le valute virtuali e valute aventi corso legale (c.d. exchanger) e i prestatori di servizi di portafoglio digitale (c.d. custodial wallet).

Il 12 novembre 2018 è stata pubblicata nella Gazzetta ufficiale dell'UE la direttiva 2018/1673 relativa alla lotta contro il riciclaggio di capitali mediante il diritto penale (GU L 284/22), cd VI Direttiva AML.

La direttiva mira a colmare alcune lacune nella definizione e nel regime sanzionatorio (penale) del riciclaggio di denaro in tutta l'Unione europea. Inoltre, il nuovo quadro giuridico facilita la cooperazione giudiziaria e di polizia nella lotta contro il riciclaggio di denaro e il finanziamento del terrorismo.

Il D.Lgs. 184/2021, oltre ad avere modificato il testo dei delitti di indebito utilizzo di carte di credito e di frode informatica, ha anche inserito nel codice penale il nuovo art. 493-quater.

La Legge 18 Marzo 2008, n. 48, ha introdotto nel corpus del D.Lgs. n. 231/2001 l'art. 24 bis, modificato da ultimo dal D.Lgs. 15 gennaio 2016 n. 17, estendendo così la responsabilità degli enti anche ai reati informatici reati informatici, di trattamento illecito di dati, nonché reati commessi con violazione delle prescrizioni in materia di cyber security:

- falsità in documenti informatici (art. 491 bis c.p.);
- accesso abusivo ad un sistema informatico o telematico (art. 615 ter c.p.);
- detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615 quater c.p.);
- diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico e telematico (art. 615 quinquies c.p.);
- intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617 quater c.p.);
- installazione di apparecchiature atte ad intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617 quinquies c.p.);
- danneggiamento di informazioni, dati e programmi informatici (art. 635 bis c.p.);
- danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità (art. 635 ter c.p.);
- danneggiamento di sistemi informatici o telematici (art. 635 quater c.p.);
- danneggiamento di sistemi informatici o telematici di pubblica utilità (art. 635 quinquies c.p.);
- frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640 quinquies c.p.).
- delitti di cui all'articolo 1, comma 11, del decreto-legge 21 settembre 2019, n. 105 (convertito nella legge n. 133 del 2019).

Il D.Lgs. n. 81 del 9 aprile 2008 recante "Attuazione dell'articolo 1 della legge 3 agosto 2007, n. 123, in materia di tutela della salute e della sicurezza nei luoghi di lavoro", riformula l'art. 25 septies introdotto dalla Legge 3 agosto 2007 n.123 che estendeva la responsabilità degli enti ai delitti di omicidio colposo (art. 589 c.p.) e lesioni

colpose grave e gravissime (art. 590 comma terzo c.p.) commesse in violazione delle norme sulla sicurezza e tutela della salute nei luoghi di lavoro
La Legge 15 luglio 2009, n. 94, recante "Disposizioni in materia di sicurezza pubblica", ha introdotto i reati in materia di criminalità organizzata, di cui al nuovo art. 24-ter:

- associazione per delinquere (art. 416 c.p.);
- associazione per delinquere finalizzata alla riduzione o al mantenimento in schiavitù, alla tratta di persone, all'acquisto e alienazione di schiavi ed ai reati concernenti le violazioni delle disposizioni sull'immigrazione clandestina di cui all'art. 12 D.Lgs. n. 286/1998 (art. 416 comma 6 c.p.);
- associazione per delinquere finalizzata al compimento di reati di prostituzione minorile, pornografia minorile, detenzione di materiale pornografico, pornografia virtuale, iniziative turistiche volte allo sfruttamento della prostituzione minorile, violenza sessuale, atti sessuali con minorenni, corruzione di minorenne, violenza sessuale di gruppo, adescamento di minorenni, quando detti illeciti sono commessi ai danni di minorenni (art. 416, comma 7, c.p.);
- associazioni di tipo mafioso anche straniere (art. 416 bis c.p.);
- scambio elettorale politico mafioso (art. 416 ter c.p.);
- sequestro di persona a scopo di estorsione (art. 630 c.p.);
- delitti commessi avvalendosi delle condizioni previste dall'articolo 416- bis ovvero al fine di agevolare l'attività delle associazioni previste dallo stesso articolo;
- associazione per delinquere finalizzata allo spaccio di sostanze stupefacenti o psicotrope (art. 74 del Testo Unico di cui al Decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);
- delitti concernenti la fabbricazione ed il traffico di armi da guerra, esplosivi ed armi clandestine (di cui all'articolo 407, comma 2, lettera a), numero 5), del codice di procedura penale).

La Legge 23 luglio 2009, n. 99, recante "Disposizioni per lo sviluppo e l'internazionalizzazione delle imprese, nonché in materia di energia" ha ha disposto (con l'art. 15, comma 7, lettera a) la modifica dell'art. 25-bis, commi 1, 2, l'introduzione della lettera f-bis) e la modifica della rubrica.
Pertanto, tale articolo, nella sua attuale formulazione, reca la disciplina in materia di reati di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, prevedendo quali reati presupposto:

- falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.);
- alterazione di monete (art. 454 c.p.);
- contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.);
- fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.);
- spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.);
- spendita di monete falsificate ricevute in buona fede (art. 457 c.p.);
- uso di valori di bollo contraffatti o alterati (art. 464 commi 1 e 2 c.p.);
- falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.);
- contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.);
- introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

La medesima Legge n. 99/2009 ha poi ha disposto (con l'art. 15, comma 7, lettera b) l'introduzione dell'art. 25-bis.1. in materia di reati contro l'industria ed il commercio, il quale prevede i seguenti reati presupposto:

- turbata libertà dell'industria o del commercio (art. 513 c.p.);
- illecita concorrenza con minaccia o violenza (art. 513 bis c.p.);
- frodi contro le industrie nazionali (art. 514 c.p.);

- frode nell'esercizio del commercio (art. 515 c.p.);
- vendita di sostanze alimentari non genuine come genuine (art. 516c.p.);
- vendita di prodotti industriali con segni mendaci (art. 517 c.p.);
- fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art.517 ter c.p.);
- contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517 quater c.p.).

Da ultimo, ancora la Legge n. 99/2009, come modificata dalla Legge 3 agosto 2009, n. 116 (in G.U. 14/08/2009 n. 188) e, da ultimo, dal D.Lgs. 7 luglio 2011, n. 121 (in G.U. 01/08/2011n. 177) ha introdotto l'art. 25 novies del D.Lgs 231/2001 in materia di violazione della legge sul diritto d'autore, prevedendo i seguenti reati:

- messa a disposizione del pubblico, in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta, o di parte di essa (art. 171, L. n. 633/1941 comma 1 lett. a) bis);
- reati di cui al punto precedente commessi su opere altrui non destinate alla pubblicazione qualora ne risulti offeso l'onore o la reputazione (art. 171, L. n. 633/1941 comma 3);
- abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita o detenzione a scopo commerciale o imprenditoriale o concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per rimuovere o eludere i dispositivi di protezione di programmi per elaboratori (art. 171 bis L. n. 633/1941 comma 1);
- riproduzione, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico, del contenuto di una banca dati; estrazione o reimpiego della banca dati; distribuzione, vendita o concessione in locazione di banche dati (art. 171 bis L. n. 633/1941 comma 2);
- abusiva duplicazione, riproduzione, trasmissione o diffusione in pubblico con qualsiasi procedimento, in tutto o in parte, di opere dell'ingegno destinate al circuito televisivo, cinematografico, della vendita o del noleggio di dischi, nastri o supporti analoghi o ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento; opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico musicali, multimediali, anche se inserite in opere collettive o composite o banche dati; riproduzione, duplicazione, trasmissione o diffusione abusiva di oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi; immissione in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, di un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa (art. 171 ter L. n. 633/1941);
- mancata comunicazione alla SIAE dei dati di identificazione dei supporti non soggetti al contrassegno o falsa dichiarazione (art. 171 septies L. n. 633/1941);
- fraudolenta produzione, vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico e privato di apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale (art. 171 octies L. n. 633/1941).

La Legge 3 Agosto 2009, n. 166 di ratifica della Convenzione ONU sulla corruzione del 31.10.2003 ha introdotto il reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria (art. 377 bis c.p.), di cui al nuovo art. 25-decies.

Hanno in seguito avuto impatto sul corpus del D.Lgs. 231/2001 i seguenti provvedimenti normativi:
D.Lgs. n. 106 del 3 agosto 2009 recante Disposizioni integrative e correttive del D.Lgs. n. 81 del 9 aprile 2008, in materia di tutela della salute e della sicurezza nei luoghi di lavoro;

D.Lgs. n. 39 del 27 gennaio 2010 (Attuazione della direttiva 2006/43/CE, relativa alle revisioni legali dei conti annuali e dei conti consolidati) recante l'abrogazione e la modifica di reati presupposto dell'illecito amministrativo di cui all'articolo 25-ter del D.Lgs. 231/2001;

Legge n. 96 del 4 giugno 2010 recante Disposizioni per l'adempimento di obblighi derivanti dall'appartenenza dell'Italia alle Comunità europee - Legge Comunitaria 200; Legge n. 122 del 30 luglio 2010 recante Misure urgenti in materia di stabilizzazione finanziaria e di competitività economica;

Legge n. 136 del 13 agosto 2010 recante Piano straordinario contro le mafie, nonché delega al governo in materia di normativa antimafia.

Successivamente, il D.lgs. 121/2011, in vigore dal 16 agosto 2011, ha introdotto nel novero dei reati di cui al Decreto anche i reati in materia ambientale (art. 25 undecies):

- uccisione, distruzione, cattura, prelievo, detenzione di esemplari appartenenti ad una specie animale e/o vegetale selvatica protetta (c.p. art. 727 bis);
- distruzione o deterioramento di habitat all'interno di un sito protetto (c.p. art. 733 bis);
- scarico di acque reflue industriali contenenti sostanze pericolose (D.Lgs. 152/06 art. 137 comma 1);
- scarico di acque reflue industriali contenenti sostanze pericolose in violazione delle prescrizioni imposte con l'autorizzazione o dalle Autorità competenti (D.Lgs. 152/06 art. 132, comma 2);
- scarico di acque reflue industriali contenenti sostanze pericolose in violazione dei limiti tabellari o dei limiti più restrittivi fissati da Regioni o Province autonome o dall'Autorità competente (D.Lgs. 152/06 art.137, comma 5, primo e secondo periodo);
- violazione dei divieti di scarico al suolo, nelle acque sotterranee, nel suolo o nel sottosuolo (D.Lgs. 152/06 art.137, comma 11);
- scarico in mare da parte di navi o aeromobili di sostanze o materiali di cui è vietato lo sversamento, salvo in quantità minime e autorizzato dall'Autorità competente (D.Lgs. 152/06 art. 137, comma 13);
- attività di gestione di rifiuti non autorizzata (D.Lgs. 152/06 art.256, comma 1);
- realizzazione e gestione di discarica non autorizzata (D.Lgs. 152/06 art. 256, comma 3, primo periodo);
- attività non consentita di miscelazione di rifiuti (D.Lgs. 152/06 art. 256, comma 5);
- deposito irregolare presso il luogo di produzione di rifiuti sanitari pericolosi (D.Lgs. 152/06 art.256, comma 6);
- omessa bonifica (D.Lgs. 152/06 art. 257); • violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari (D.Lgs. 152/06 art. 258, comma 4);
- predisposizione di un certificato di rifiuti falso, utilizzato nell'ambito del sistema di tracciabilità SISTRI (D.Lgs. 152/06, art. 260 bis, comma 6) ;
- trasporto di rifiuti pericolosi senza la copia cartacea della scheda SISTRI-AREA MOVIMENTAZIONE o senza certificato analitico dei rifiuti, nonché uso di certificato di analisi contenente informazioni false circa i rifiuti trasportati in ambito SISTRI (D.Lgs. 152/06, art. 260 bis comma 7, secondo periodo e terzo periodo) ;
- trasporto di rifiuti con copia cartacea della scheda SISTRI-AREA MOVIMENTAZIONE fraudolentemente alterata (D.Lgs. 152/06, art. 260 bis comma 8, primo e secondo periodo) ;
- traffico illecito di rifiuti (D.Lgs. 152/06, art. 259);
- attività organizzate per il traffico illecito di rifiuti (D.Lgs. 152/06, art. 260); • attività organizzate per il traffico illecito di rifiuti ad alta radioattività (D.Lgs. 152/06, art. 260 comma 2);
- violazione, nell'esercizio di uno stabilimento, dei valori limite di emissione o delle prescrizioni stabilite dall'autorizzazione, dai piani e programmi o dalla normativa, ovvero dall'Autorità competente, che determini anche il superamento dei valori limite di qualità dell'aria previsti dalla vigente normativa (D.Lgs. 152/06, art. 279, comma 5);
- importazione, esportazione, o riesportazione di esemplari appartenenti a specie animali e vegetali in via di estinzione (allegato A Reg. CE 338/97), senza il prescritto certificato o licenza o con certificato o licenza non validi o in violazione dell'osservanza delle prescrizioni finalizzate all'incolumità degli esemplari (L.150/92, art. 1);
- importazione, esportazione o riesportazione di esemplari appartenenti a specie animali e vegetali in via di estinzione (allegati B e C del Reg. CE 338/97), senza il prescritto certificato o licenza o con

certificato o licenza non validi o omissione dell'osservanza delle prescrizioni finalizzate all'incolumità degli esemplari (L. 150/92, art. 2);
- falsificazione o alterazione di certificati e licenze; notifiche di importazione, comunicazioni o dichiarazioni al fine di acquisire un certificato o una licenza; uso di certificati e licenze falsi o alterati per l'importazione di animali e vegetali in via di estinzione (L. 150/92, art. 3 bis, comma 1);
- detenzione di esemplari vivi di mammiferi e rettili di specie selvatica o riprodotti in cattività, che costituiscono pericolo per la salute e per l'incolumità pubblica (L. 150/92, art. 6, co. 4);
- violazione delle disposizioni che prevedono la cessazione e la riduzione dell'impiego (produzione, utilizzazione, commercializzazione, importazione ed esportazione) di sostanze nocive per lo strato di ozono (Legge n° 549 del 1993, art. 3, comma 6);
- sversamento doloso in mare di sostanze inquinanti (D.Lgs. 202/07, art. 8);
- sversamento colposo in mare di sostanze inquinanti (D.Lgs. 202/07, art. 9);
- inquinamento ambientale (art. 452 bis c.p.);
- disastro ambientale (art. 452 quater c.p.);
- delitti colposi contro l'ambiente (art. 452 quinquies c.p.);
- traffico ed abbandono di materiale ad alta radioattività (art. 452 sexies c.p.);
- delitti associativi aggravati dalla finalità di commettere un reato ambientale (art. 452 octies c.p.).

Il D.Lgs. 16 luglio 2012, n. 109 ha introdotto nel corpus del Decreto l'art. 25-duodecies, che sanziona il delitto di impiego di cittadini di paesi terzi il cui soggiorno è irregolare, previsto dall'art. 22, comma 12-bis, D.Lgs. 25 luglio 1998, n. 286.

La Legge n. 190 del 6 novembre 2012, in vigore dal 28 novembre 2012, ha inserito all'art. 25 del Decreto il reato di "induzione indebita a dare o promettere utilità" (art. 319-quater c.p.) e all'art. 25-ter dello stesso il reato di corruzione tra privati (art. 2635 c.c.).

La legge n. 186 del 15 dicembre 2014, in vigore dal 1° gennaio 2015, ha inserito tra i reati presupposto richiamati dall'art. 25-octies del Decreto l'art. 648-ter.1 c.p., che punisce il delitto di autoriciclaggio.

La Legge 22 Maggio 2015, n. 68, entrata in vigore in data 29 maggio 2015, ha modificato l'art. 25-undecies, inserendo nei reati presupposto dello stesso nuove fattispecie di delitti ambientali (inquinamento ambientale, disastro ambientale, inquinamento ambientale e disastro ambientale commessi con colpa ai sensi dell'art. 452-quinquies c.p., delitti associativi (ovvero associazione per delinquere ed associazione di tipo mafioso) aggravati ai sensi dell'art. 452 – octies c.p., traffico e abbandono di materiale ad alta radioattività).

La Legge 30 Maggio 2015, n. 69, ha modificato l'art. 25-ter del Decreto e ha previsto alcune modifiche agli artt. 2621 e 2622 c.c..

La Legge 16 marzo 2006, n. 146, artt. 3 e 10, ha esteso la responsabilità degli enti anche alle ipotesi di commissione dei c.d. reati transnazionali ossia i reati puniti con la pena della reclusione non inferiore nel massimo a quattro anni coinvolgenti un gruppo criminale organizzato e commessi (i) in più di uno stato; (ii) in uno Stato ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato; (iii) in uno Stato ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato; (iv) in uno Stato ma abbia effetti sostanziali in un altro Stato.

La Legge n. 179 del 30 novembre 2017, ha introdotto "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". L'art. 2 della predetta legge ha modificato profondamente l'art. 6 del D. Lgs. 231/2001, introducendo i commi 2 bis, 2 ter e 2 quater.

Il D. Lgs. n. 38/2017, in vigore dal 14 aprile 2017, recante la riforma del reato di corruzione tra privati e l'introduzione del reato di istigazione alla corruzione tra privati.

La Legge n. 161/2017 ha modificato l'art. 25 duodecies del Decreto in tema di impiego di cittadini di paesi terzi il cui soggiorno è irregolare (art. 22 comma 12 bis D.Lgs. 286/1998).

La Legge n. 167/2017 è intervenuta sul Decreto introducendo l'art. 25-terdecies disciplinante il reato di propaganda ed istigazione a delinquere per motivi di discriminazione razziale, etnica e religiosa (L. n. 654/1975, art. 3 comma 3 bis).

La Legge n. 3 del 9 gennaio 2019, pubblicata sulla Gazzetta Ufficiale n. 13 del 16 gennaio 2019, si pone quale finalità principale il contrasto alle diverse forme di corruzione, sia in ambito pubblico che tra privati.

L'art. 25 del Decreto, rubricato "Concussione, induzione indebita a dare o promettere utilità e corruzione tra privati", è stato così riformato:

1) il novero dei reati presupposto è stato ulteriormente ampliato con l'introduzione al comma 1 del reato di "traffico di influenze illecite" (art. 346 bis c.p.), a sua volta interessato da un'importante riforma sia in termini di estensione del perimetro della fattispecie sia in termini di inasprimento della pena che dalla reclusione da uno a tre anni passa alla reclusione da uno a quattro anni e sei mesi;
2) la sanzione interdittiva prevista per i reati di cui ai commi 2 e 3 dell'art. 25 è stata inasprita: se ante riforma era prevista una durata non inferiore ad un anno, ora la sanzione interdittiva avrà durata "non inferiore a quattro anni e non superiore a sette anni" ove il reato presupposto sia stato commesso da un soggetto apicale, ovvero durata "non inferiore a due anni e non superiore a quattro anni" ove il reato presupposto sia stato, invece, commesso da un soggetto sottoposto alla direzione e controllo del soggetto apicale;
3) al comma 5 bis è stata introdotta una sanzione interdittiva attenuata ("non inferiore a tre mesi e non superiore a due anni") nel caso in cui prima della sentenza di primo grado l'Ente si sia efficacemente adoperato per evitare che l'attività delittuosa sia portata a conseguenze ulteriori, per assicurare le prove dei reati e per l'individuazione dei responsabili ovvero per il sequestro delle somme o altre utilità e abbia eliminato le carenze organizzative che hanno determinato il reato mediante l'adozione e l'attuazione di modelli organizzativi idonei a prevenire reati della specie di quello verificatosi.
4) la previsione della procedibilità d'ufficio per i reati di corruzione tra privati e di istigazione alla corruzione tra privati.

Con la legge 3 maggio 2019, n. 39 è stata data attuazione, nel nostro ordinamento, alla Convenzione del Consiglio d'Europa sulla manipolazione di competizioni sportive, fatta a Magglingen il 18 settembre 2014. L'art. 5, comma 1, della legge in questione inserisce nel D.Lgs. 231/2001, il nuovo art. 25-quaterdecies rubricato "Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati". Alla luce di ciò, l'Ente può rispondere per i reati di "Frode in competizioni sportive" (art. 1 legge 13/12/1989 n. 401) e di "Esercizio abusivo di attività di giuoco o di scommessa" (art. 4 legge 13/12/1989 n. 401). Tenendo conto dei criteri di cui all'art. 11 D. Lgs. 231/2001 «della gravità del fatto, del grado della responsabilità dell'ente nonché dell'attività svolta per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti» all'ente si può irrogare la sanzione pecuniaria fino a € 67.080 (260 quote) per le contravvenzioni e fino a € 774.500 (500 quote) per i delitti.

L'art. 1 del D.L. n.105 del 21 Settembre 2019 che, coordinato con Legge di conversione n.133 del 18 Novembre 2019, ha istituito il "perimetro di sicurezza nazionale cibernetica" al fine di assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori, pubblici e privati aventi una sede nel territorio nazionale, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il mantenimento di attività' civili, sociali o economiche fondamentali per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale. Tutto ciò ha

comportato la modifica dell'Art. 24-bis del D.Lgs. 231/01 recante reati informatici e di trattamento illecito di dati.

Il nuovo Art. 25-quinquiesdecies contempla i seguenti reati tributari:

- Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (Articolo 2 del D.L.gs 74 modificato al comma 1, con l'aggiunta del comma 2-bis.);
- Dichiarazione fraudolenta mediante altri artifici (Articolo 3 del D.L.gs 74 modificato al comma 1);
- Emissione di fatture o altri documenti per operazioni inesistenti (Articolo 8 del D.L.gs 74 modificato al comma 1 e aggiunta del comma 2-bis);
- Occultamento o distruzione di documenti contabili (Articolo 10 del D.L.gs 74 modificato al comma 1);
- Sottrazione fraudolenta al pagamento di imposte (Articolo 11 del D.L.gs 74).

Con il Decreto Legislativo n. 75 del 14 luglio 2020 è stata recepita nell'ordinamento italiano, la Direttiva (UE) 2017/1371 (cd. Direttiva PIF – Protezione Interessi Finanziari) del Parlamento europeo e del Consiglio del 5 luglio 2017, recante norme per la "lotta contro la frode che lede gli interessi finanziari dell'Unione mediante il diritto penale".

Innanzitutto, viene estesa la responsabilità 231 per i reati di frode nelle pubbliche forniture, ex art. 356 c.p. e frode ai danni del Fondo Europeo Agricolo di Garanzia e del Fondo Europeo Agricolo per lo Sviluppo, ex art. 2, comma 1, L. 898/1986. Le nuove disposizioni sono inserite nell'art. 24 D.Lgs. 231/2001 (che prevede una sanzione fino a 500 quote o da 250 a 600 in caso di profitto e danno ingente, nonché sanzioni interdittive, esclusa la chiusura dell'attività e la revoca o sospensione di autorizzazioni). In relazione a tutti i delitti contro la pubblica amministrazione previsti dall'art. 24, inoltre, la responsabilità è allargata anche ai casi che vedono danneggiati non solo lo Stato e gli enti pubblici italiani, ma anche l'Unione Europea. All'art. 25 del D.Lgs. 231/2001 sono aggiunti peculato (art. 314, c.1, c.p. con l'esclusione dell'ipotesi di uso momentaneo del bene), peculato mediante profitto dell'errore altrui (art. 316 c.p.) e abuso d'ufficio (art. 323 c.p.).

La sanzione prevista per l'ente consiste in una pena pecuniaria fino a 250 quote. L'art. 25-quinquesdecies, introdotto dal Decreto fiscale, vedrà ora un nuovo comma 1bis, che comporta la punibilità delle società per le gravi frodi Iva (carattere transazionale ed evasione non inferiore a 10milioni di euro) in ipotesi di dichiarazione infedele (art. 4 D.Lgs. 74/2000, sanzione pecuniaria fino a 300 quote), omessa dichiarazione (art. 5, sanzione pecuniaria fino a 400 quote) e indebita compensazione (art. 10quater, sanzione pecuniaria fino a 400 quote). Per tali nuove fattispecie si applicheranno la circostanza aggravante e le sanzioni interdittive già disciplinate dall'art. 25quinquesdecies.

Il D.Lgs. 75/2020, oltre ad avere ampliato il novero dei reati tributari e dei reati contro la Pubblica Amministrazione presenti nell'elenco dei "reati presupposto", ha inserito anche i reati di contrabbando (doganale), tramite l'articolo 25 sexiesdecies del D.Lgs. 231/2001, che prevede sanzioni pecuniarie fino a 200 quote (o fino a 400 al superamento della soglia di 100mila euro) e interdittive (esclusa la chiusura dell'attività e la revoca o sospensione di autorizzazioni) per i reati di cui al "Testo Unico delle disposizioni legislative in materia doganale" (D.P.R. 43/1973), il quale enuclea numerose fattispecie nel Titolo VII (Violazioni doganali), Capi I (Contrabbando) e II (Contravvenzioni e illeciti amministrativi).

Il 29 novembre 2021 è stato pubblicato in Gazzetta Ufficiale il D.Lgs. 184/2021, recante l'"Attuazione della direttiva (UE) 2019/713 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".

In particolare, l'art. 3, in vigore a partire dal prossimo 14 dicembre 2021, introduce nel D.Lgs. 231/2001 il nuovo art. 25-octies.1 in materia di "Delitti in materia di strumenti di pagamento diversi dai contanti".

Il Catalogo dei reati presupposto alla responsabilità delle persone giuridiche viene quindi esteso anche all'art. 493-ter c.p. (indebito utilizzo e falsificazione di carte di credito e di pagamento), all'art. 493-quater c.p.

(detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti) e all'art. 640-ter c.p. (frode informatica), quest'ultimo non solo se commesso ai danni dello Stato o di altro ente pubblico o dell'Unione Europea, come già previsto dall'art. 24 del Decreto, ma anche "nell'ipotesi aggravata dalla realizzazione di un trasferimento di denaro, di valore monetario o di valuta virtuale".

Il 25 febbraio 2022 è stato pubblicato in Gazzetta Ufficiale il decreto-legge n. 13/2022, recante «Misure urgenti per il contrasto alle frodi e per la sicurezza nei luoghi di lavoro in materia edilizia, nonché sull'elettricità prodotta da impianti da fonti rinnovabili» (c.d. Decreto Frodi), volto a rafforzare il contrasto alle frodi in materia di erogazioni pubbliche, alla luce delle recenti notizie di operazioni illecite aventi ad oggetto le agevolazioni fiscali note come "superbonus".

L'art. 2 del decreto, recante "Misure sanzionatorie contro le frodi in materia di erogazioni pubbliche", ha modificato in senso ampliativo la rubrica ed il testo degli artt. 240-bis, 316-bis e 316-ter del codice penale. Ed invero:

- all'articolo 240-bis, primo comma, dopo le parole: «629,» sono inserite le seguenti: «640, secondo comma, n. 1, con l'esclusione dell'ipotesi in cui il fatto è commesso col pretesto di far esonerare taluno dal servizio militare, 640-bis,». Viene quindi esteso il numero dei reati per i quali può essere disposta la c.d. confisca in casi particolari;
- all'articolo 316-bis c.p.: nella rubrica, le parole «a danno dello Stato» sono sostituite dalle seguenti: «di erogazioni pubbliche»; al primo comma, le parole da «o finanziamenti» a «finalità» sono sostituite dalle seguenti: «, finanziamenti, mutui agevolati o altre erogazioni dello stesso tipo, comunque denominate, destinati alla realizzazione di una o più finalità, non li destina alle finalità previste»;
- all'articolo 316-ter: nella rubrica, le parole «a danno dello Stato» sono sostituite dalla seguente: «pubbliche»; al primo comma, dopo la parola: «contributi,» è inserita la seguente: «sovvenzioni,»;
- all'articolo 640-bis, dopo la parola: «contributi,» è inserita la seguente: «sovvenzioni,».
- Seppur indirettamente, il decreto in esame incide anche sul catalogo dei reati presupposto della responsabilità degli enti, in ragione della modifica dei reati di cui agli arti. 316 bis, 316 ter e 640 bis c.p. richiamati dall'art. 24 del D. Lgs. 231/2001.

Nel corso dei primi mesi del 2022, ulteriori novità legislative sono intervenute a modificare il dettato normativo del D. Lgs. n. 231/2001, modificando ed allargando le maglie di alcune fattispecie incluse nel catalogo dei reati presupposto.

In questo contesto, di particolare interesse risultano essere le previsioni di cui alla Legge n. 238/2021 recante "Disposizioni per l'adempimento degli obblighi derivanti dall'appartenenza dell'Italia all'Unione Europea - Legge Europea 20192020". Nello specifico, le linee di intervento sono state le seguenti:

- adeguamento alla direttiva n. 2013/40/UE relativa agli attacchi contro i sistemi di informazione - modifica degli artt. 615 e ss. c.p., richiamati dall'art. 24-bis del D.lgs. 231/2001;
- adeguamento alla direttiva n. 2011/93/UE relativa alla lotta contro l'abuso e lo sfruttamento sessuale dei minori e la pornografia minorile – modifica degli artt. 600-quater e 609-undecies c.p., presupposto della responsabilità degli enti ex art. 25-quinquies del D.lgs. 231/2001;
- modifiche alle fattispecie in materia di abusi di mercato, richiamate dall'art. 25-sexies del D.lgs. 231/2001 in risposta ad una procedura di infrazione avviata contro l'Italia.

Con riferimento alla prima direttrice, si segnalano le modifiche apportate a talune fattispecie richiamate come reati presupposto dall'art. 24-bis del D.lgs. 231/2001, dedicato ai "Delitti informatici e trattamento illecito di dati".

In particolare, l'articolo 615-quater c.p. vede una nuova rubricazione, un ampliamento delle condotte punibili e una modificazione in termini di cornice edittale. La nuova disposizione, rubricata ora "Detenzione, diffusione

e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici", prevede che sia punibile il soggetto che "abusivamente si procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparati, strumenti, parti di apparati o di strumenti idonei all'accesso ad un sistema informatico o telematico protetto da misure di sicurezza al fine di arrecare a sé o ad altri un profitto o di arrecare ad altri un danno". La pena della reclusione si estende sino a due anni nell'ipotesi base, mentre da uno a tre anni se ricorre una delle circostanze di cui all'articolo 617-quater comma 4.

L'articolo 615-quinquies c.p. ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico" e così come modificato dalla suddetta legge, si connota per una nuova formulazione della condotta punibile ora rivolta a "Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, abusivamente si procura, detiene, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette in altro modo a disposizione di altri o installa apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329".

Con riferimento all'art. 617-quater c.p., vengono inasprite le pene per l'ipotesi di cui al primo comma ora punita con la reclusione "da un anno e sei mesi a cinque anni", nonché di quella prevista dal comma quarto per la quale si prevede un innalzamento della pena edittale "da tre a otto anni". L'articolo 617-quinquies ora rubricato "Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche" si connota per una nuova formulazione relativa alle condotte punibili che prevedono ora l'attivazione della risposta sanzionatoria nei confronti di chiunque "procura, detiene, produce, riproduce, diffonde, importa, comunica, consegna, mette in altro modo a disposizione di altri o installa apparecchiature, programmi, codici, parole chiave o altri mezzi atti ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi" con il fine di "intercettare comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero di impedirle o interromperle".

Infine, l'articolo 26 della legge 238/2021 introduce alcune modifiche ad alcuni reati richiamati dall'art. 25 sexies del D.lgs. 231/2001 "Reati di abuso di mercato". In particolare, l''articolo 184 T.U.F. ora rubricato "Abuso o comunicazione illecita di informazioni privilegiate. Raccomandazione o induzione di altri alla commissione di abuso di informazioni privilegiate", vede:

- un inasprimento delle pene per i c.d. insider primari e per i c.d. criminal insider: la pena della reclusione viene innalzata fino a due anni nel minimo e dodici anni nel massimo, unitamente alla previsione di una multa da 20.000 euro a 3 milioni di euro;
- la definitiva introduzione della punibilità dell'insider secondario con la previsione della pena della reclusione da un anno e sei mesi fino a dieci anni e la multa da 20.000 euro a 2,5 milioni di euro, salvi i casi di concorso con gli insider primari in cui si applicheranno le sanzioni loro riferite e l'estensione dell'aggravante ex 184, comma 3, T.U.F. viene estesa allo stesso insider secondario
- un aumento di pena della multa fino al triplo o fino al maggior importo di dieci volte il prodotto o il profitto conseguito dal reato quando, per la rilevante offensività del fatto, per le qualità personali del colpevole o per l'entità del prodotto o del profitto conseguito dal reato, essa appare inadeguata anche se applicata nel massimo;
- l'applicazione delle disposizioni dell'articolo anche ai fatti che riguardano condotte od operazioni, comprese le offerte, relative alle aste su una piattaforma d'asta autorizzata, come un mercato regolamentato di quote di emissioni o di altri prodotti oggetto d'asta correlati, anche quando i prodotti oggetto d'asta non sono strumenti finanziari, ai sensi del regolamento (UE) n. 1031/2010 della Commissione, del 12 novembre 2010. Rispetto all'art. 185 T.U.F. "Manipolazione del mercato" vengono abrogati i commi 2-bis e 2-ter. Infine, l'ambito di applicazione della confisca obbligatoria

viene ora limitato al solo profitto del reato di abuso o comunicazione illecita di informazioni privilegiate o manipolazione di mercato e non anche ai mezzi usati per commettere il reato.

Inoltre, il 3 marzo 2022, la Camera dei deputati ha approvato in via definitiva il disegno di legge che modifica il Codice penale, inasprendo le sanzioni per i reati contro il paesaggio e i beni culturali, ora espressamente richiamati anche dal D. Lgs. 231/2001. Tra le principali novità, si evidenziano:

- introduzione del nuovo titolo VIII-bis, dedicato ai "Delitti contro il patrimonio culturale" all'interno del Codice penale i cui nuovi articoli disciplinano, con pene più severe rispetto a quelle previste per i corrispondenti delitti semplici, il furto, l'appropriazione indebita, la ricettazione, il riciclaggio, l'autoriciclaggio e il danneggiamento che abbiano ad oggetto beni culturali;
- l'introduzione nel Codice penale dei reati di autoriciclaggio di beni culturali e di furto di beni culturali;
- l'applicazione delle disposizioni penali a tutela dei beni culturali anche ai fatti commessi all'estero in danno del patrimonio culturale nazionale;
- la conferma della confisca obbligatoria, anche per equivalente, per le cose che hanno costituito oggetto del reato, a meno che appartengano a persona estranea al reato;
- l'estensione il catalogo dei delitti per cui è consentita la confisca allargata, a seguito dell'inserimento del reato di ricettazione dei beni culturali, del reato di impiego di beni culturali provenienti da delitto, del reato di riciclaggio e di autoriciclaggio di beni culturali.

Infine, si segnala l'introduzione delle nuove fattispecie contro il patrimonio culturale anche nel catalogo dei reati presupposto ex D.lgs. 231/2001, con la previsione di sanzioni fino a 900 quote e l'applicabilità sanzioni interdittive per una durata massima di due anni.

1.4 Delitti tentati

La responsabilità della società può conseguire non soltanto allorché si siano verificati tutti gli elementi costitutivi della fattispecie di reato (es. gli atti fraudolenti, l'induzione in errore, il profitto e il danno, nel reato di truffa), ma anche nell'ipotesi in cui il reato non si sia completamente consumato - per mancato compimento dell'azione, o per mancata verificazione dell'evento - rimanendo allo stadio del solo tentativo (ricorrendo tali presupposti la pena inflitta alla persona fisica e le eventuali conseguenze sanzionatorie per la società, in presenza dei criteri di ascrizione della responsabilità subiranno soltanto una riduzione ex art. 26 d.lgs. 231/01).

1.5 Le sanzioni

Il Decreto 231 prevede che agli enti possano essere applicate sanzioni pecuniarie e sanzioni interdittive. In particolare, nel settore finanziario è previsto l'intervento della Banca d'Italia sia con un ruolo di collaborazione con il pubblico ministero e con il giudice del procedimento penale, sia con l'incarico di porre in essere l'esecuzione delle eventuali sanzioni interdittive disposte nei confronti di un intermediario finanziario, di cui all'art. 9, comma 2, lettere a) – interdizione dall'esercizio dell'attività e b) – sospensione o revoca dall'autorizzazione.

Le sanzioni pecuniarie si applicano ogniqualvolta un ente commetta uno degli illeciti previsti dal Decreto 231, mentre quelle interdittive possono essere applicate solo in relazione ai reati per i quali sono espressamente previste dal Decreto 231, qualora ricorra almeno una delle seguenti condizioni:

- l'ente ha tratto dal reato un profitto di rilevante entità ed il reato è stato commesso:
  (i) da soggetti in posizione apicale, ovvero
  (ii) da soggetti sottoposti all'altrui direzione e vigilanza quando la commissione del reato è stata determinata o agevolata da gravi carenze organizzative;
  in caso di reiterazione degli illeciti.

Ai fini della quantificazione delle sanzioni pecuniarie il giudice deve tenere conto:

- della gravità del fatto;
- del grado di responsabilità dell'ente;
- dell'attività svolta dall'ente per eliminare o attenuare le conseguenze del fatto e per prevenire la commissione di ulteriori illeciti;
- delle condizioni economiche e patrimoniali dell'ente.

Le sanzioni interdittive applicabili agli enti ai sensi del Decreto 231 sono:

- l'interdizione dall'esercizio dell'attività;
- la sospensione o revoca di autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;
- il divieto di contrattare con la pubblica amministrazione, salvo che per ottenere le prestazioni di pubblico servizio;
- la esclusione da agevolazioni, finanziamenti, contributi o sussidi e nella revoca di quelli già concessi;
- il divieto di pubblicizzare beni e servizi.

Il tipo e la durata delle sanzioni interdittive sono stabiliti dal giudice sulla base dei criteri indicati per la commisurazione delle sanzioni pecuniarie. Il Decreto 231 prevede, inoltre, la possibilità applicare alcune sanzioni in via definitiva (quindi superando il limite massimo di durata), qualora si verifichino determinati eventi considerati particolarmente gravi.

Con specifico riferimento al settore finanziario, le sanzioni interdittive non possono essere applicate in via cautelare agli intermediari finanziari. La stessa norma stabilisce, altresì, un flusso informativo tra il Pubblico Ministero che iscrive nel registro delle notizie di reato un illecito amministrativo a carico di un intermediario finanziario e la Banca d'Italia e la Consob, le quali possono essere sentite nel corso del procedimento ed hanno, in ogni caso la facoltà di presentare relazioni scritte.

Il giudice può disporre, in luogo dell'applicazione della sanzione interdittiva, la prosecuzione dell'attività dell'ente da parte di un commissario per un periodo pari alla durata della pena interdittiva che sarebbe stata applicata, qualora ricorra almeno una delle seguenti condizioni:

- l'ente svolge un pubblico servizio o un servizio di pubblica necessità la cui interruzione può provocare un grave pregiudizio alla collettività;

- l'interruzione dell'attività dell'ente può provocare, tenuto conto delle sue dimensioni e delle condizioni economiche del territorio in cui è situato, rilevanti ripercussioni sull'occupazione.

Oltre alle predette sanzioni, il Decreto 231 prevede che venga sempre disposta la confisca del prezzo o del profitto del reato, che può avvenire anche per equivalente, nonché la pubblicazione della sentenza di condanna in presenza di una sanzione interdittiva.

1.6 L'efficace attuazione del Modello quale possibile esimente dalla responsabilità

Un aspetto fondamentale delineato dal Decreto è l'innovativo concetto di Modello di organizzazione e gestione, idoneo a prevenire i reati sopra elencati.

L'importanza di tale documento è notevole, se si considera che, come detto, ai sensi dell'art. 6 del D. Lgs. 231/01, l'ente non incorre in responsabilità se, tra l'altro, "**l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi**".

In pratica, il Legislatore ha inteso legare la responsabilità dell'ente alla mancata osservanza di regole di organizzazione, previamente definite, la cui corretta applicazione consenta di minimizzare il rischio di commissione del reato; di conseguenza, l'adozione del Modello è di indubbia utilità nel prevenire la commissione di reati, nonché la loro reiterazione.

A ciò si aggiunga, inoltre, che il Modello può spiegare la propria efficacia anche se introdotto successivamente alla commissione del reato. Al riguardo:

- nel caso in cui il reato sia già stato commesso ed il Modello non ancora predisposto, se il Modello viene adottato prima del dibattimento di primo grado, lo stesso può concorrere ad evitare all'ente l'applicazione delle più gravi sanzioni interdittive (art. 17, lett. b), nonché una sensibile riduzione delle pene pecuniarie (art. 12, comma 2, lett. b, e comma 3);
- l'adozione del Modello può avvenire anche a sentenza di condanna già emessa, al fine di ottenere la conversione delle sanzioni interdittive ex art. 78; a patto che, oltre alla concorrenza delle altre condizioni previste dall'art. 17, se ne documenti l'adozione entro 20 giorni dalla notifica della sentenza.

In definitiva, l'adozione di un Modello, preventiva o successiva alla commissione di un reato da parte della società, può avere ripercussioni sia sull'*an* (cioè sulla concreta applicazione), che sulla natura (cioè sulla tipologia) stessa delle sanzioni.

2. L'ADOZIONE DEL MODELLO DA PARTE DI CONFIDI SYSTEMA!

2.1 Gli obiettivi perseguiti da Confidi Systema! con l'adozione del Modello

Il presente Modello si integra all'interno della normativa, delle procedure e dei sistemi di controllo già esistenti ed operanti in Confidi Systema!

Il contesto organizzativo della Società è costituito dall'insieme di regole, strutture e procedure che ne garantiscono il corretto funzionamento; si tratta dunque di un sistema estremamente articolato che rappresenta già di per sé uno strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli Enti.

Come anticipato, l'adozione del Modello non è obbligatoria; la scelta di Confidi Systema! è fondata, tuttavia, sulla convinzione che l'efficacia di un idoneo Modello non rilevi solo in virtù della possibilità di esonero dalla responsabilità dell'ente, ma migliori l'efficienza stessa dell'intero sistema societario, determinando, altresì, una maggiore competitività rispetto ai concorrenti.

Infatti se l'adozione e la diffusione del Modello mira da un lato a determinare una piena consapevolezza nel potenziale autore del reato di commettere un illecito (la cui commissione è fortemente condannata e contraria agli interessi di Confidi Systema!, anche quando apparentemente quest'ultima potrebbe trarne un vantaggio), dall'altro, grazie ad un costante monitoraggio dell'attività, mira a consentire a Confidi Systema! di prevenire o reagire tempestivamente al fine di impedire la commissione del reato stesso.

La Società è ferma nel ritenere che un idoneo Modello di organizzazione e gestione possa sensibilizzare tutti i dipendenti, collaboratori e terzi in genere all'adozione di comportamenti corretti nell'espletamento delle proprie attività, in modo tale da prevenire il rischio di commissione dei reati tassativamente previsti dal Decreto o la loro reiterazione. In particolare, la finalità del Modello è quella di:

- adeguarsi alla normativa sulla responsabilità amministrativa degli Enti, ancorché il Decreto non ne abbia imposto l'obbligatorietà;
- verificare e valorizzare i presidi già in essere, atti a scongiurare condotte illecite rilevanti ai sensi del Decreto;
- informare tutto il personale della Società della portata della normativa e delle severe sanzioni che
- possono ricadere sulla stessa Società nell'ipotesi di perpetrazione degli illeciti richiamati dal Decreto;
- rendere noto a tutto il personale che si stigmatizza ogni condotta contraria a disposizioni di legge, regolamenti, norme di vigilanza, regole aziendali interne, nonché ai principi di sana e corretta gestione delle attività societarie cui la Società si ispira;
- informare tutto il personale della Società dell'esigenza di un puntuale rispetto delle disposizioni contenuta nel Modello stesso, la cui violazione è punita con severe sanzioni disciplinari;

- informare i collaboratori esterni, i consulenti e i partner della Società della portata della normativa, nonché dei principi etici e delle norme comportamentali adottate da Confidi Systema! ed imporre agli stessi il rispetto dei valori etici cui quest'ultima si ispira;
- informare i collaboratori esterni, i consulenti ed i partner della Società che si stigmatizza ogni condotta contraria a disposizioni di legge, regolamenti, norme di vigilanza, regole aziendali interne, nonché ai principi di sana e corretta gestione dell'attività societaria cui Confidi Systema! si ispira;
- informare i collaboratori esterni, i consulenti ed i partner della Società delle gravose sanzioni amministrative applicabili a Confidi Systema! nel caso di commissione degli illeciti di cui al Decreto;
- compiere ogni sforzo possibile per prevenire gli illeciti nello svolgimento delle attività sociali, mediante un'azione di monitoraggio continuo sulle aree a rischio, attraverso una sistematica attività di formazione del personale sulla corretta modalità di svolgimento dei propri compiti e mediante un tempestivo intervento per prevenire e contrastare la commissione di illeciti.

2.2 Le fasi di realizzazione del Modello

Nel corso della realizzazione del proprio Modello, Confidi Systema! ha svolto un'intensa attività, articolata nelle fasi descritte nel documento relativo alla mappatura delle attività aziendali e metodologia adottata, cui si rimanda[2].

2.3 Raccolta e analisi della documentazione

Nel corso di tale fase, Confidi Systema! si è concentrata preliminarmente sulla raccolta e, successivamente, sull'analisi della seguente documentazione:

- Statuto;
- Organigramma e funzionigramma;
- Codice interno di comportamento e regolamento della società;
- Regolamenti operativi e procedure formalizzate;
- Piano delle verifiche della funzione Internal Audit;
- Piano delle verifiche della funzione Compliance;
- Piano delle attività della Funzione Antiriciclaggio;
- Contratti e Convenzioni;
- Relazioni sulla Struttura Organizzativa;
- Documenti concernenti il Bilancio.

2.4 Identificazione delle attività a rischio

Tale attività è stata attuata attraverso l'analisi della struttura aziendale, allo scopo di individuare le modalità operative, la ripartizione delle competenze e la sussistenza, o l'insussistenza, e la misurazione di rischi di commissione di ciascuna ipotesi di reato indicata dalla legge.

Al fine di poter identificare le aree aziendali a rischio di commissione dei reati rilevanti ai sensi del D. Lgs. 231/01, sono state condotte interviste dirette ai responsabili di ciascuna singola area aziendale ed i risultati delle interviste sono stati documentati in sintetiche schede descrittive.

A conclusione di tale fase, dall'analisi delle risposte fornite in sede di intervista, è emersa la sussistenza di taluni profili di rischio di commissione di ipotesi di reato individuate dalla legge.

[2] All. ConfidiSystema!_Risk Assessment 231

Successivamente, si è proceduto alla mappatura delle "aree cd sensibili" prevalentemente su base documentale.

Non sono stati presi in considerazione, perché **non attinenti alle attività esercitate da Confidi Systema!** o perché rientranti nella sfera del "rischio accettabile", i seguenti reati previsti dal Decreto:

- delitti di criminalità organizzata;
- delitti contro l'industria e il commercio;
- delitti con finalità di terrorismo o di eversione dell'ordine democratico;
- pratiche di mutilazione degli organi genitali femminili;
- delitti contro la personalità individuale;
- reati transnazionali;
- delitti in materia di violazione del diritto di autore;
- impiego di cittadini di paesi il cui soggiorno è irregolare;
- i delitti in materia di strumenti di pagamento diversi dai contanti;
- i reati ambientali;
- i reati di razzismo e xenofobia;
- i reati di frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati;
- il contrabbando;
- i delitti contro il patrimonio culturale.

2.5 Identificazione e analisi degli attuali presidi al rischio

Tale attività ha avuto lo scopo di individuare, tramite interviste dirette ai responsabili delle aree aziendali a rischio, le procedure operative e i concreti controlli esistenti e idonei a presidiare il rischio individuato. Anche il risultato di tale attività è stato documentato in schede e/o documenti.

2.6 Gap analysis

In seguito all'identificazione ed all'analisi dei presidi al rischio già presenti, Confidi Systema! si è concentrata proprio sul confronto tra la situazione di rischio e detti presidi, con le esigenze e i requisiti imposti dal D. Lgs. 231/01, al fine di individuare le carenze del sistema esistente. È stato, pertanto, richiesto, al soggetto responsabile della gestione delle attività a rischio non sufficientemente presidiate, di identificare interventi idonei a prevenire in concreto le identificate ipotesi di rischio.

2.7 Esiti Risk Assessment

L'attività di Risk Assessment, conclusasi a settembre 2022, ha individuato n. **13** aree sensibili 231/01 e n. **56** attività potenzialmente collegate al rischio di commissione dei reati previsti dal Decreto Legislativo 231/01 (cd. «reati presupposto»). Poiché ad ogni attività può essere associato più di un reato presupposto, sono stati individuati n. **71** rischi 231.

A ciascuna attività mappata è stato associato un **rischio lordo**. Considerata la frequenza dell'attività e il suo impatto, non sono stati individuati rischi lordi «bassi» ma soltanto «alti» e «medi», così distribuiti:

- n. 45 rischi lordi classificati di livello ALTO;
- n. 26 rischi lordi classificati di livello MEDIO.

Sulla base della valutazione dei presidi e delle attività di mitigazione già poste in essere nella gestione dei processi, i **rischi netti** sono stati pertanto classificati come segue:

- **Non è stato individuato alcun rischio netto di livello ALTO**.

- **n. 69 rischi netti classificati di livello BASSO**. I controlli/presidi posti in essere dalla Società hanno determinato un sensibile abbassamento del rating del rischio lordo non richiedendo ulteriori attività di mitigazione;
- **n.2 rischi netti classificati di livello MEDIO**. Sebbene il rischio lordo sia in parte mitigato dai presidi in essere, sono state identificate ulteriori attività di mitigazione.

Confidi Systema! ha ritenuto pertanto che l'adozione del **Codice Etico**, dei principi generali di controllo interno, delle linee di condotta, delle specifiche procedure/policy e l'istituzione di dettagliati flussi informativi verso l'O.D.V., siano adeguati a prevenire le condotte illecite relative ai reati presupposti per tutti i rischi netti classificati di livello basso.

Per quanto riguarda invece i **2 rischi netti classificati di livello medio**, riscontrato che allo stato i presidi esistenti da soli non garantiscono un livello di protezione sufficiente, Confidi Systema! mediante l'adozione di specifici protocolli ha inteso mitigare i rischi ad essi connessi.

3. Redazione e diffusione del Modello organizzativo e gestionale

Nell'ultima fase, l'attività di Confidi Systema! si è concentrata sulla revisione del Modello di Organizzazione e Gestione, la cui struttura verrà descritta al successivo paragrafo, unitamente alla diffusione del documento.

3.1 La struttura del Modello della Società

Il Modello della Società contempla pertanto il coordinato funzionamento di un articolato sistema piramidale di principi e procedure che si può descrivere sinteticamente come segue:

- **Codice Etico**: è l'insieme dei principi generali (trasparenza, correttezza, lealtà) cui si ispira lo svolgimento e la conduzione degli affari nell'ambito di un più generale percorso di crescita sostenibile garantendo, nel contempo, l'efficienza e l'efficacia del Sistema di controllo interno.

- **Sistema di controllo interno:** è l'insieme degli "strumenti", attività, processi e strutture organizzative volti a fornire una ragionevole garanzia in ordine al raggiungimento degli obiettivi di efficienza e di efficacia operativa, affidabilità delle informazioni finanziarie e gestionali, rispetto delle leggi e dei regolamenti, nonché salvaguardia del patrimonio sociale anche contro possibili frodi. Il sistema di controllo interno si fonda e si qualifica su alcuni principi generali, appositamente definiti nell'ambito del Modello il cui campo di applicazione si estende trasversalmente a tutti i diversi livelli organizzativi (Direzione Generale, Aree, Funzioni, Uffici).

- **Linee di condotta:** introducono regole specifiche al fine di evitare la costituzione di situazioni ambientali favorevoli alla commissione di reati in genere, e tra questi in particolare dei reati e degli illeciti amministrativi rilevanti ai sensi del Decreto. Talune regole sono altresì specifiche per la gestione dei rapporti con i rappresentanti della Pubblica Amministrazione e con i terzi in generale, nonché per gli adempimenti e le attività di natura societaria e di comunicazione al mercato.

- **Presidi organizzativi**: per lo più esplicitati nelle procedure adottate da Confidi Systema!, sono stati elaborati per tutti i processi operativi di medio rischio (l'attività di Risk Assessment 231 svolta ha infatti escluso, come detto, la presenza di processi di alto rischio netto) e per i processi strumentali. Tali schemi presentano un'analoga struttura che si sostanzia in un complesso di regole volte ad individuare le principali fasi di ogni processo, le specifiche attività di controllo per prevenire ragionevolmente i correlati rischi di reato, nonché appositi flussi informativi[7] verso l'Organismo di Vigilanza ("OdV", il cui ruolo è di seguito meglio dettagliato) al fine di evidenziare situazioni di eventuale inosservanza delle procedure stabilite nei modelli di organizzazione. Gli schemi di controllo interno sono stati elaborati alla luce di tre regole cardine e precisamente:

1. la **separazione dei ruoli** nello svolgimento delle attività inerenti ai processi;

2. la c.d. "**tracciabilità" delle scelte**, cioè la costante visibilità delle stesse (ad es. mediante apposite evidenze documentali), per consentire l'individuazione di precisi "punti" di responsabilità e la "motivazione" delle scelte stesse;

3. **l'oggettivazione dei processi decisionali**, nel senso di prevedere che, nell'assumere decisioni, si prescinda da valutazioni meramente soggettive, facendosi invece riferimento a criteri precostituiti.

L'Organismo di Vigilanza, il Collegio Sindacale, l'Internal Audit, la Compliance e la società di revisione esterna nello svolgimento della propria attività e per quanto di propria competenza, hanno accesso diretto, completo, ed incondizionato a tutte le persone, attività, operazioni, documenti, archivi e beni aziendali.

3.2 Linee di condotta

Il presente paragrafo contiene le "Linee di Condotta" alle quali Amministratori, Sindaci, dirigenti, dipendenti, consulenti, collaboratori e in generale tutti coloro che operano per conto o in favore di Confidi Systema! o che con lo stesso intrattengono relazioni di affari ("Destinatari delle Linee di Condotta"), ciascuno nell'ambito delle proprie funzioni e responsabilità, devono attenersi per evitare il determinarsi di situazioni ambientali favorevoli alla commissione di fatti illeciti in genere, e tra questi in particolare dei reati rilevanti ai sensi del Decreto.

Le Linee di Condotta individuano, se pur a titolo non esaustivo, comportamenti relativi all'area del "fare" e del "non fare", con riferimento in particolare ai rapporti con la Pubblica Amministrazione, con i soggetti terzi, nonché alle attività e agli adempimenti societari, specificando in chiave operativa quanto espresso dai principi del Codice Etico.

“Area del fare”

I Destinatari delle Linee di Condotta sono impegnati al rispetto delle leggi e dei regolamenti vigenti in Italia. I Destinatari delle Linee di Condotta sono impegnati al rispetto delle procedure aziendali e si ispirano ai principi del Codice Etico in ogni decisione o azione attinente alla gestione della Società.

I responsabili delle aree devono curare che:

- per quanto ragionevolmente possibile, tutti i dipendenti siano edotti sulla normativa e sui comportamenti conseguenti e, qualora abbiano dei dubbi sulle modalità da seguire, siano adeguatamente indirizzati;
- sia attuato un adeguato programma di formazione e sensibilizzazione continua sulle problematiche attinenti al Codice Etico.

Linee di Condotta nei rapporti con la P.A.

Nell’eventuale partecipazione a gare indette dalla Pubblica Amministrazione e in generale in ogni trattativa con questa, i Destinatari delle Linee di Condotta devono operare nel rispetto delle leggi, dei regolamenti vigenti e della correttezza professionale.

I responsabili delle aree che hanno correntemente attività di contatto con la Pubblica Amministrazione devono:

- fornire ai propri collaboratori direttive sulle modalità di condotta operativa da seguire nei contatti formali ed informali intrattenuti con i diversi soggetti pubblici, secondo le peculiarità del proprio ambito di attività, trasferendo conoscenza della normativa e consapevolezza delle situazioni a rischio di reato;
- prevedere adeguati meccanismi di tracciabilità circa i flussi comunicativi/informativi verso la Pubblica Amministrazione.

Quando vengono richiesti allo Stato o ad altro ente pubblico o alle Comunità europee contributi, sovvenzioni o finanziamenti, tutti i Destinatari delle Linee di Condotta coinvolti in tali procedure devono:

- attenersi ai principi di correttezza, utilizzando e presentando dichiarazioni e documenti veritieri, completi e attinenti le attività per le quali i benefici possono essere legittimamente ottenuti;
- una volta ottenute le erogazioni richieste, destinarle alle finalità per le quali sono state richieste e concesse.

Linee di Condotta in materia societaria

I componenti del Consiglio di Amministrazione, il Direttore Generale e Vice Direttore Generale, per quanto di rispettiva competenza, e le persone sottoposte alla loro vigilanza e, in generale, chiunque si occupi a qualunque titolo della redazione del bilancio sono tenuti alla piena osservanza della normativa aziendale e, in particolare, sono vincolati al rispetto delle procedure, delle istruzioni e delle norme operative di dettaglio in materia di redazione del bilancio e regolamentazione dei principali processi aziendali.

Il Responsabile dell’Area Amministrazione, nell’ambito dei compiti assegnati e per quanto di propria competenza, deve curare che ogni operazione sia:

- legittima, congrua, autorizzata e verificabile;
- correttamente ed adeguatamente registrata sì da rendere possibile la verifica del processo di decisione, autorizzazione e svolgimento;

- corredata di un supporto documentale idoneo a consentire, in ogni momento, i controlli sulle caratteristiche e motivazioni dell'operazione e l'individuazione di chi ha autorizzato, effettuato, registrato, verificato l'operazione stessa.

I Destinatari delle Linee di Condotta coinvolti nelle attività di formazione del bilancio o di altri documenti similari devono comportarsi correttamente, prestare la massima collaborazione, garantire la completezza e la chiarezza delle informazioni fornite, l'accuratezza dei dati e delle elaborazioni, segnalare eventuali conflitti di interesse, ecc.

I componenti del Consiglio di Amministrazione, in conformità con quanto previsto dalla Procedura Conflitti d'interesse e operazioni con Parti Correlate adottata da Confidi Systema!, comunicano al CdA ed al Collegio Sindacale ogni interesse che, per conto proprio o di terzi, abbiano in una determinata operazione della Società, precisandone la natura, i termini, l'origine e la portata; se si tratta di Direttore Generale, deve altresì astenersi dal compiere l'operazione, investendo della stessa l'organo collegiale.

I Destinatari delle Linee di Condotta e in particolare gli Amministratori:

- nella redazione del bilancio o di altri documenti similari devono rappresentare la situazione economica, patrimoniale o finanziaria con verità, chiarezza e completezza;
- devono rispettare puntualmente le richieste di informazioni da parte del Collegio Sindacale e facilitare in ogni modo lo svolgimento delle attività di controllo legalmente attribuite ai soci e ad altri organi sociali;
- fornire agli Organi di Vigilanza informazioni corrette e complete sulla situazione economica, patrimoniale o finanziaria.

Possono tenere contatti con la stampa solo i soggetti a ciò autorizzati e questi devono diffondere notizie sulla Società rispondenti al vero nel rispetto delle leggi e dei regolamenti vigenti.

Linee di Condotta nei rapporti con soggetti interni e terzi alla Società

I Destinatari delle Linee di Condotta sono tenuti al rispetto delle leggi e dei regolamenti vigenti in Italia; non dovrà essere iniziato o proseguito alcun rapporto con chi non intenda rispettare tale principio.

L'incarico per operare in nome e/o per conto e/o nell'interesse della Società deve essere conferito in forma scritta e deve prevedere una specifica clausola che vincoli l'incaricato all'osservanza dei principi etico-comportamentali adottati dalla Società.

Il mancato rispetto di specifica clausola potrà permettere alla Società di risolvere il rapporto contrattuale. Tutti i consulenti, i fornitori e, in generale, qualunque soggetto terzo che agisca in nome e/o per conto e/o nell'interesse della Società sono individuati e selezionati con assoluta imparzialità, autonomia e indipendenza di giudizio. Nella loro selezione la Società ha cura di valutare la loro competenza, reputazione, indipendenza, capacità organizzativa e idoneità alla corretta e puntuale esecuzione delle obbligazioni contrattuali e degli incarichi affidati.

Tutti i consulenti e gli altri soggetti che prestano servizio presso la Società devono operare, sempre e senza eccezioni, con integrità e diligenza, nel pieno rispetto di tutti i principi di correttezza e liceità previsti dai codici etici dagli stessi eventualmente adottati.

“Area del non fare”

È fatto divieto ai Destinatari delle Linee di Condotta di compiere, anche in forma associata, qualunque atto che sia o possa essere considerato contrario a leggi e/o a regolamenti vigenti, anche nel caso in cui da tale comportamento derivi o possa, anche solo in astratto, derivare un qualunque vantaggio o configurarsi un interesse per la Società.

I Destinatari delle Linee di Condotta sono tenuti a evitare qualunque situazione di conflitto di interessi con la Società, obbligandosi nel caso in cui la situazione di conflitto comunque si verifichi a segnalarlo immediatamente alla stessa Società.

I Destinatari delle Linee di Condotta devono astenersi da qualunque comportamento lesivo dell’immagine della Società.

Linee di Condotta nei rapporti con la P.A. e l’Unione Europea

Nei rapporti con rappresentanti della Pubblica Amministrazione, sia italiani che esteri, è fatto divieto di:

- per i Consulenti e Collaboratori, promettere od offrire ai rappresentanti della P.A. o dell’Unione Europea (oppure a persone

a questi “vicine” o “gradite”) denaro, doni o altra utilità in nome e/o per conto della Società;

- per gli Amministratori, Dipendenti e Dirigenti promettere od offrire ai rappresentanti della P.A. o dell’Unione Europea (oppure a persone a questi “vicine” o “gradite”) denaro, doni o altra utilità in elusione delle procedure societarie;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell’immagine aziendale;
- promettere o fornire, anche tramite “terzi”, lavori/servizi di utilità personale (ad es. opere di ristrutturazione di edifici da loro posseduti o goduti – o posseduti o goduti da loro parenti, affini, conviventi amici, ecc.);
- fornire o promettere di fornire, sollecitare od ottenere informazioni e/o documenti riservati o comunque tali da poter compromettere l’integrità o la reputazione di una od entrambe le parti;
- favorire, nei processi d’acquisto, fornitori e sub-fornitori in quanto indicati dai rappresentanti stessi della Pubblica Amministrazione o dell’Unione Europea come condizione per lo svolgimento successivo delle attività (ad es. affidamento della commessa, concessione del finanziamento agevolato, concessione della licenza).

Tali azioni e comportamenti sono vietati se fatti sia direttamente dalla Società tramite i suoi dipendenti, sia tramite persone non dipendenti che agiscano in nome e/o per conto e/o nell’interesse di questa.

Inoltre, nei confronti della Pubblica Amministrazione o dell’Unione Europea, è fatto divieto di:

- esibire documenti/dati falsi od alterati;
- sottrarre od omettere documenti veri;
- tenere una condotta ingannevole che possa indurre la Pubblica Amministrazione in errore nella valutazione tecnico-economica dei prodotti e servizi offerti/forniti;
- omettere informazioni dovute, al fine di orientare indebitamente a proprio favore le decisioni della Pubblica Amministrazione o dell’Unione Europea;
- tenere comportamenti comunque intesi ad influenzare indebitamente le decisioni della Pubblica Amministrazione o dell’Unione Europea;
- abusare della posizione di incaricato di pubblico servizio per ottenere utilità a vantaggio personale o della Società;
- abusare della posizione di incaricato di pubblico servizio per indurre indebitamente altri a dare o promettere per sé o per altri denaro o altra utilità.

In conformità e nei limiti delle disposizioni normative vigenti, è fatto divieto di assumere o conferire incarichi di consulenza alle dipendenze della Società a ex dipendenti della Pubblica Amministrazione che abbiano partecipato personalmente e attivamente a una trattativa d'affari o abbiano avallato le richieste effettuate alla Pubblica Amministrazione o dell'Unione Europea dalla Società o da società controllate, collegate della medesima o sottoposte a comune controllo con la medesima.

Nel corso dei processi civili, penali o amministrativi, è fatto divieto di intraprendere, direttamente o indirettamente, alcuna azione illecita che possa favorire o danneggiare una delle parti in causa.

È fatto divieto a chiunque, in qualsiasi forma e con qualsiasi modalità, nel malinteso interesse della Società, di coartare la volontà dei Destinatari di rispondere all'Autorità giudiziaria o indurre di avvalersi della facoltà di non rispondere.

Nei rapporti con l'Autorità giudiziaria è vietata ogni forma di condizionamento che induca il Destinatario a rendere dichiarazioni non veritiere, in particolare in relazione alle dichiarazioni da rendere, al Destinatario non è consentito altresì accettare denaro o altra utilità, anche attraverso terzi.

Linee di Condotta nei rapporti con soggetti interni e terzi alla Società

In generale è fatto divieto di:

- per i Consulenti e Collaboratori, promettere od offrire denaro, doni o altra utilità in nome e/o per conto della Società;
- per gli Amministratori, Dipendenti e Dirigenti promettere od offrire denaro, doni o altra utilità in elusione delle procedure societarie;
- effettuare spese di rappresentanza ingiustificate e con finalità diverse dalla mera promozione dell'immagine aziendale;
- promettere o fornire, anche tramite "terzi", lavori/servizi di utilità personale;
- fornire o promettere di fornire, sollecitare od ottenere informazioni e/o documenti riservati o comunque tali da poter compromettere l'integrità o la reputazione di una od entrambe le parti;
- favorire, nei processi d'acquisto, fornitori e sub-fornitori in quanto indicati dai soggetti come sopra individuati come condizione per lo svolgimento successivo delle attività (ad es. affidamento della commessa).

Tali azioni e comportamenti sono vietati se fatti sia direttamente dalla Società tramite i suoi dipendenti, sia tramite persone non dipendenti che agiscano in nome e/o per conto e/o nell'interesse di questa.

3.3 Principi generali dei presidi organizzativi

Il sistema di controllo interno è definito come l'insieme dei "processi" presidiati dal Consiglio di Amministrazione, dal management e dagli altri membri della struttura aziendale, che si prefigge di fornire una ragionevole certezza in merito al conseguimento dei seguenti obiettivi:

- efficacia ed efficienza delle attività operative;
- affidabilità delle informazioni e del reporting economico/finanziario;
- conformità alle leggi, ai regolamenti alle norme e procedure interne;
- salvaguardia del patrimonio aziendale.

Il Sistema di Controllo Interno si articola in principi generali il cui campo di applicazione si estende con continuità attraverso i diversi livelli organizzativi.

Ambiente di controllo

I poteri di rappresentanza sono conferiti definendo i limiti in relazione alle dimensioni normali delle operazioni inerenti e secondo ambiti di esercizio strettamente collegati alle mansioni assegnate ed alla struttura organizzativa.

Le responsabilità devono essere definite e debitamente distribuite evitando sovrapposizioni funzionali o allocazioni operative che concentrino le attività critiche su un unico soggetto.

Tutte le operazioni sono poste in essere secondo le modalità previste dai regolamenti interni ed in particolare dal Regolamento poteri e deleghe. I perimetri operativi di ciascuna area sono inoltre definiti ed esplicitati nella Relazione sulla Struttura Organizzativa che viene redatta con cadenza annuale secondo quanto previsto dalla normativa vigente.

I sistemi operativi devono essere coerenti con il Codice Etico.
In particolare, le informazioni finanziarie della Società devono essere predisposte:

- nel rispetto delle leggi e dei regolamenti, dei principi contabili statuiti e delle "best practice" internazionali;
- in coerenza con le procedure amministrative definite;
- nell'ambito di un completo ed aggiornato piano dei conti.

Valutazione dei rischi

Gli obiettivi di ciascuna Area aziendale devono essere adeguatamente definiti e comunicati a tutti i livelli interessati per rendere chiaro e condiviso l'orientamento generale della stessa al fine anche di consentire l'individuazione dei rischi connessi al raggiungimento degli obiettivi, prevedendone periodicamente un adeguato monitoraggio ed aggiornamento.
Gli eventi negativi che possono minacciare la continuità operativa devono essere oggetto di apposita attività di valutazione dei rischi e di adeguamento delle protezioni.

I processi di innovazione relativi a prodotti/servizi, organizzazioni e sistemi devono prevedere un'adeguata valutazione dei rischi realizzativi.

Attività di controllo

I processi operativi devono essere definiti prevedendo un adeguato supporto documentale (policy, norme operative, regolamenti interni, ecc.) e/o di sistema per consentire che siano sempre verificabili in termini di congruità, coerenza e responsabilità.
Le scelte operative devono essere tracciabili in termini di caratteristiche e motivazioni e devono essere individuabili coloro che hanno autorizzato, effettuato e verificato le singole attività.

Lo scambio di informazioni fra fasi/processi contigui deve prevedere meccanismi (riconciliazioni, quadrature, ecc.) per garantire l'integrità e la completezza dei dati gestiti.
Le risorse umane devono essere selezionate, assunte e gestite secondo criteri di trasparenza e in coerenza con i valori etici e gli obiettivi definiti dall'azienda.

Devono essere periodicamente analizzate le conoscenze e le competenze professionali disponibili nell'Area aziendale in termini di congruenza rispetto agli obiettivi assegnati.

Il personale deve essere formato e addestrato per lo svolgimento delle mansioni assegnate.

L'acquisizione di beni e servizi per il funzionamento aziendale deve avvenire sulla base di analisi dei fabbisogni e da fonti adeguatamente selezionate e monitorate.

Informazioni e Comunicazione

Deve essere previsto un adeguato sistema di indicatori per processo/attività ed un relativo flusso periodico di reporting verso il management.

I Sistemi Informativi, amministrativi e gestionali devono essere orientati all'integrazione ed alla standardizzazione.

I meccanismi di sicurezza devono garantire un'adeguata protezione/accesso fisico-logico ai dati e ai beni dell'Unità Operativa, secondo il principio "need to know-need to do".

Monitoraggio

Il sistema di controllo è soggetto ad attività di supervisione continua per valutazioni periodiche ed il costante adeguamento.

3. L'Organismo di Vigilanza

3.1 Struttura e composizione dell'Organismo di Vigilanza

Il D. Lgs. 231/01 prevede l'istituzione di un Organismo di Vigilanza interno all'Ente (OdV), dotato di autonomi poteri di iniziativa e di controllo, cui è assegnato specificamente il compito di vigilare sul funzionamento e l'osservanza del modello di organizzazione e di gestione e di curarne il relativo aggiornamento.

L'esistenza dell'OdV è uno dei requisiti necessari per l'idoneità del modello stesso.

L'OdV di Confidi Systema! è composto da 3 membri scelti tra soggetti in possesso di specifica esperienza in materie giuridiche, economiche, finanziarie o tecnico-scientifiche o comunque tra soggetti in possesso di adeguate competenze specialistiche derivanti, ad esempio, dall'aver svolto per un congruo periodo di tempo attività professionali in materie attinenti al settore finanziario e/o dall'avere una adeguata conoscenza dell'organizzazione e dei principali processi aziendali.

L'OdV è istituito con delibera del Consiglio di Amministrazione che, in sede di nomina, deve dare atto della valutazione della sussistenza dei requisiti di indipendenza, autonomia, onorabilità e professionalità dei suoi membri.
La durata in carica dei membri dell'OdV coincide con quella del Consiglio di Amministrazione che l'ha nominato e i suoi membri possono essere rieletti.

La rinuncia da parte dei componenti dell'OdV può essere esercitata in qualsiasi momento e deve essere comunicata al Consiglio di Amministrazione per iscritto unitamente alle motivazioni che l'hanno determinata.

3.2 Requisiti

- **Requisiti soggettivi di eleggibilità**

La nomina quale componente dell'OdV è condizionata alla presenza dei requisiti soggettivi di eleggibilità.

Costituiscono motivi di ineleggibilità e/o di decadenza dei componenti dell'OdV di Confidi Systema!:

- trovarsi in stato di interdizione temporanea o di sospensione dagli uffici direttivi delle persone giuridiche e delle imprese;
- trovarsi in una delle condizioni di ineleggibilità o decadenza previste dall'art. 2382 del codice civile;
- avere titolarità, diretta o indiretta, di partecipazioni azionarie di entità tale da permettere di esercitare una notevole influenza su Confidi Systema!;
- essere stato sottoposto a misure di prevenzione ai sensi del decreto legislativo 6 settembre 2011, n. 159 e successive modificazioni e integrazioni, salvi gli effetti della riabilitazione;
- aver riportato sentenza di condanna o patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione:
- per uno dei delitti previsti dal regio decreto 16 marzo 1942, n. 267 (legge fallimentare);
- per uno dei delitti previsti dal titolo XI del Libro V del codice civile (società e consorzi);
- per un delitto non colposo, per un tempo non inferiore a un anno;
- per un delitto contro la P.A., contro la fede pubblica, contro il patrimonio, contro l'economia pubblica ovvero per un delitto in materia tributaria;
- per uno dei reati previsti dalle norme che disciplinano l'attività Societaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
- aver riportato, in Italia o all'estero, sentenza di condanna o di patteggiamento, ancorché non definitiva, anche se con pena condizionalmente sospesa, salvi gli effetti della riabilitazione, per le violazioni rilevanti ai fini della responsabilità amministrativa degli enti ex D.Lgs. 231/01;
- essere destinatario di un decreto che dispone il rinvio a giudizio per tutti i reati/illeciti previsti dal D.Lgs. 231/01;
- aver svolto funzioni di amministratore esecutivo ricoperte, nei tre esercizi precedenti alla nomina quale membro dell'Organismo di Vigilanza, in imprese:
  - sottoposte a procedure concorsuali;
  - operanti nel settore creditizio, finanziario, mobiliare e assicurativo sottoposte a procedure di liquidazione coatta amministrativa o amministrazione straordinaria.

- **Autonomia e indipendenza**

L'autonomia e l'indipendenza dell'OdV sono garantite:

- dal posizionamento, indipendente da qualsiasi area, all'interno della struttura organizzativa aziendale;
- dal possesso dei requisiti di indipendenza, onorabilità e professionalità dei membri dell'OdV;
- dalle linee di riporto verso il Vertice aziendale attribuite all'OdV;
- dalla insindacabilità, da parte di alcun altro organismo o struttura aziendale, delle attività poste in essere dall'OdV;
- dall'autonomia nello stabilire le proprie regole di funzionamento mediante l'adozione di un proprio Regolamento.

L'OdV dispone di autonomi poteri di spesa sulla base di un preventivo annuale, approvato dal Consiglio di Amministrazione, su proposta dell'OdV stesso. In ogni caso, quest'ultimo può richiedere un'integrazione del budget assegnato, qualora non sufficiente all'efficace espletamento delle proprie incombenze, e può estendere la propria autonomia di spesa di propria iniziativa in presenza di situazioni eccezionali o urgenti, che saranno oggetto di successiva relazione al Consiglio di Amministrazione.

All'OdV e alla struttura della quale esso si avvale sono riconosciuti, nel corso delle verifiche ed ispezioni, i più ampi poteri al fine di svolgere efficacemente i compiti affidatigli.

Nell'esercizio delle loro funzioni i membri dell'OdV non devono trovarsi in situazioni, anche potenziali, di conflitto di interesse con Confidi Systema! derivanti da qualsivoglia ragione (ad esempio di natura personale o familiare).
In tali ipotesi essi sono tenuti ad informare immediatamente gli altri membri dell'OdV e devono astenersi dal partecipare alle relative deliberazioni.

- **Professionalità**

L'OdV deve essere composto da soggetti dotati di adeguata esperienza aziendale e delle cognizioni tecniche e giuridiche necessarie per svolgere efficacemente le attività proprie dell'Organismo.
In particolare, i componenti dell'OdV devono possedere una consistente esperienza aziendale, maturata all'interno di Confidi Systema! ovvero in società con connotazioni simili per quanto attiene l'attività svolta, e devono, altresì, ricoprire cariche dirigenziali apicali.
Ove necessario, l'OdV può avvalersi, con riferimento all'esecuzione delle operazioni tecniche necessarie per lo svolgimento della funzione di controllo, anche di consulenti esterni. In tal caso, i consulenti dovranno sempre riferire i risultati del loro operato all'OdV.

- **Continuità di azione**

L'OdV deve essere in grado di garantire la necessaria continuità nell'esercizio delle proprie funzioni, anche attraverso la programmazione e pianificazione dell'attività e dei controlli, la verbalizzazione delle riunioni e la disciplina dei flussi informativi provenienti dalle strutture aziendali.

3.3 Revoca

I membri dell'OdV possono essere revocati dal Consiglio di Amministrazione solo per giusta causa. La deliberazione di revoca è portata a conoscenza e sottoposta al previo assenso del Collegio Sindacale.

A tale proposito, per "giusta causa" di revoca si intende, a titolo esemplificativo e non limitativo:

- una grave negligenza nell'assolvimento dei compiti connessi con l'incarico;
- l'"omessa o insufficiente vigilanza" da parte dell'OdV – secondo quanto previsto dall'art. 6, comma 1, lett. d), D.Lgs. 231/01 – risultante da una sentenza di condanna, anche non passata in giudicato, emessa nei confronti di Confidi Systema! ai sensi del D.Lgs. 231/01 ovvero da sentenza di applicazione della pena su richiesta (il c.d. patteggiamento);
- l'accertamento, successivo alla nomina, che il membro dell'OdV abbia rivestito la qualifica di componente dell'OdV in seno a società nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del D.Lgs. 231/01), le sanzioni previste dall'art. 9 del del D.Lgs. 231/01, per illeciti commessi durante la loro carica;
- l'attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale incompatibili con i requisiti di "autonomia e indipendenza" e "continuità di azione" propri dell'OdV.
  In ogni caso qualsiasi provvedimento di disposizione di carattere organizzativo che riguardi un membro dell'OdV (ad es. cessazione rapporto di lavoro, spostamento ad altro incarico, licenziamento, provvedimenti disciplinari, nomina di nuovo responsabile) dovrà essere portato alla presa d'atto del Consiglio di Amministrazione per il tramite del Presidente dell'OdV;
- gravi e accertati motivi di incompatibilità che ne vanifichino l'indipendenza e l'autonomia;
- assenza ingiustificata a due o più riunioni consecutive dell'OdV, a seguito di rituale convocazione.

4.4 Cause di sospensione

Costituisce causa di sospensione dalla funzione di componente dell'OdV l'accertamento, dopo la nomina, che i componenti dell'Organismo di Vigilanza hanno rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento non definitivo, le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica.

I componenti dell'OdV debbono comunicare al CdA, sotto la loro piena responsabilità, il sopravvenire della causa di sospensione di cui sopra. Il CdA, anche in tutti gli ulteriori casi in cui viene direttamente a conoscenza del verificarsi della suddetta causa, provvede a dichiarare la sospensione del soggetto (o dei soggetti) dalla carica di componente dell'OdV.

La decisione sulla eventuale revoca dei membri sospesi deve essere oggetto di deliberazione del CdA. Il componente non revocato è reintegrato nel pieno delle funzioni.

4.5 Temporaneo impedimento

Nell'ipotesi in cui insorgano cause che impediscano, in via temporanea, ad un componente dell'OdV di svolgere le proprie funzioni o svolgerle con la necessaria autonomia ed indipendenza di giudizio, questi è tenuto a dichiarare la sussistenza dell'impedimento e, qualora esso sia dovuto ad un potenziale conflitto di interessi, la causa da cui il medesimo deriva, astenendosi dal partecipare alle sedute dell'Organismo o alla specifica delibera cui si riferisca il conflitto stesso, sino a che il predetto impedimento perduri o sia rimosso. A titolo esemplificativo, costituisce causa di temporaneo impedimento la malattia o l'infortunio che si protraggano per oltre tre mesi ed impediscano di partecipare alle riunioni dell'OdV.

Nel caso di temporaneo impedimento o in ogni altra ipotesi che determini per uno o più componenti l'impossibilità di partecipare alla riunione, l'Organismo opererà nella sua composizione ridotta, sempre che il numero dei rimanenti componenti (per i quali non sussistano le predette situazioni) non sia inferiore a tre, qualora tra questi vi sia il Presidente. In assenza del Presidente, il numero minimo dei componenti non potrà essere inferiore a due.

In tutto gli altri casi, il CdA dispone l'integrazione temporanea dell'Organismo di Vigilanza, nominando uno o più membri nel corso della prima seduta utile, il cui incarico avrà una durata pari al periodo di impedimento. Resta salva la facoltà per il CdA, quando l'impedimento si protragga per un periodo superiore a sei mesi, prorogabile di ulteriori 6, di addivenire alla revoca del o dei componenti per i quali si siano verificate le predette cause di impedimento.

4.6 Definizione dei compiti e dei poteri dell'Organismo di Vigilanza

L'attività di verifica e di controllo svolta dall'OdV è strettamente funzionale agli obiettivi di efficace attuazione del Modello e non va a surrogare o sostituire le funzioni di controllo istituzionali Confidi Systema!.

I compiti dell'OdV sono espressamente definiti dal D.Lgs. 231/01 al suo art. 6, comma 1, lett. b) come segue:

- vigilare su funzionamento e osservanza del Modello;
- curarne l'aggiornamento.

In adempimento a siffatti compiti, all'OdV sono affidate le seguenti attività:

- vigilare sul funzionamento del Modello rispetto alla prevenzione della commissione dei reati richiamati dal D.Lgs. 231/01;

- verificare il rispetto del Modello e dei protocolli decisionali, rilevando gli eventuali comportamenti anomali che dovessero emergere dall'analisi dei flussi informativi e dalle segnalazioni alle quali sono tenuti i destinatari del Modello;
- svolgere periodica attività ispettiva e di controllo, di carattere continuativo e ogni volta lo ritenga necessario, in considerazione dei vari settori di intervento o delle tipologie di attività e dei loro punti critici al fine di verificare l'efficienza e l'efficacia del Modello;

Inoltre, con specifico riguardo alla disciplina sul sistema interno di segnalazione (cd. "whistleblowing"):

- verificare l'adeguatezza dei canali informativi, predisposti in applicazione della disciplina sul whistleblowing, affinché gli stessi siano tali da assicurare la corretta segnalazione dei reati o delle irregolarità da parte dei dipendenti della società e nell'assicurare la riservatezza di questi ultimi nell'intero processo di gestione della segnalazione;
- verificare il soddisfacimento dell'adozione del canale informatico di cui alla lettera b) del nuovo comma 2-bis dell'art. 6 Decreto 231;
- gestire il processo di analisi e valutazione della segnalazione;
- vigilare sul rispetto del divieto di "atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione" (art. 6, comma 2-bis, lett. c, del Decreto 231), che la nuova disciplina correda di un impianto sanzionatorio da integrare nel sistema disciplinare ex art. 6, comma 2, lett. e, del Decreto 231.
- vigilare sul corretto utilizzo dei canali informativi da parte dei segnalanti.

Nello svolgimento delle proprie attività, l'OdV può:

- accedere liberamente, anche per il tramite di strutture appositamente incaricate, a qualsiasi struttura di Confidi Systema! – senza necessità di alcun consenso preventivo – per richiedere ed acquisire informazioni, documentazione e dati, ritenuti necessari per lo svolgimento dei propri compiti. Nel caso in cui venga opposto un motivato diniego all'accesso agli atti, l'OdV redige, qualora non concordi con la motivazione opposta, un rapporto da trasmettere al CdA;
- richiedere informazioni rilevanti o l'esibizione di documenti, anche informatici, pertinenti alle attività a rischio, agli amministratori, agli organi di controllo, alle società di revisione, ai collaboratori, ai consulenti ed in generale a tutti coloro che operano per conto di Confidi Systema!;
- sviluppare e promuovere il costante aggiornamento del Modello, inclusa l'identificazione, la mappatura e la classificazione delle attività a rischio formulando, ove necessario, al CdA le proposte per eventuali integrazioni e adeguamenti che si dovessero rendere necessari in conseguenza di:
- significative violazioni delle prescrizioni del Modello;
- significative modificazioni dell'assetto interno di Confidi Systema! e/o delle modalità di svolgimento dell'impresa;
- modifiche legislative al D.Lgs. 231/01, quali ad esempio introduzione di fattispecie di reato che potenzialmente hanno un impatto sul Modello della Società;
- definire e curare il flusso informativo che consenta all'OdV di essere periodicamente aggiornato dai referenti aziendali, al fine di individuare possibili carenze nel funzionamento del Modello e/o possibili violazioni dello stesso;
- attuare un efficace flusso informativo che consenta all'OdV di riferire agli organi sociali competenti in merito all'efficacia e all'osservanza del Modello;
- verificare la predisposizione di un efficace sistema di comunicazione interna per consentire la trasmissione di notizie rilevanti ai fini del D.Lgs. 231/01, garantendo la tutela e riservatezza del segnalante e promuovendo la conoscenza delle condotte che devono essere segnalate e le modalità di effettuazione delle segnalazioni;
- chiedere e ottenere informazioni dagli OdV delle società controllate;
- promuovere iniziative per la diffusione della conoscenza e della comprensione del Modello, dei contenuti del D.Lgs. 231/01, degli impatti della normativa sull'attività della Società, nonché iniziative per la formazione del personale e la sensibilizzazione dello stesso all'osservanza del Modello;

- promuovere e coordinare le iniziative volte ad agevolare la conoscenza e la comprensione del Modello da parte di tutti coloro che operano per conto di Confidi Systema!;
- fornire pareri in merito al significato ed all'applicazione delle previsioni contenute nel Modello, alla corretta applicazione dei protocolli e delle relative procedure di attuazione;
- formulare e sottoporre all'approvazione dell'organo dirigente la previsione di spesa necessaria al corretto svolgimento dei compiti assegnati, con assoluta indipendenza;
- segnalare tempestivamente all'organo dirigente, per gli opportuni provvedimenti, le violazioni accertate del Modello che possano comportare l'insorgere di una responsabilità in capo a Società e proporre le eventuali sanzioni;
- verificare l'idoneità del sistema disciplinare ai sensi e per gli effetti del D.Lgs. 231/01.

Nello svolgimento della propria attività, l'OdV, si avvale di una struttura organizzativa dedicata come definita in normativa interna e può ricorrere ad ogni altra struttura interna della società competente per le attività e/o i settori di intervento.
Il CdA dà incarico all'OdV di curare l'adeguata comunicazione alle strutture aziendali del Modello, dei compiti dell'OdV e dei suoi poteri.

I componenti dell'OdV, nonché i soggetti dei quali l'OdV stesso, a qualsiasi titolo, si avvale, sono tenuti a rispettare l'obbligo di riservatezza su tutte le informazioni delle quali sono venuti a conoscenza nell'esercizio delle loro funzioni (fatte salve le attività di reporting al CdA).

I componenti dell'OdV assicurano la riservatezza delle informazioni di cui vengano in possesso, in particolare se relative a segnalazioni che agli stessi dovessero pervenire in ordine a presunte violazioni del Modello. I componenti dell'Organismo di Vigilanza si astengono dal ricevere e utilizzare informazioni riservate per fini diversi da quelli compresi nel presente paragrafo, e comunque per scopi non conformi alle funzioni proprie dell'Organismo di Vigilanza, fatto salvo il caso di espressa e consapevole autorizzazione.

Ogni informazione in possesso dei componenti dell'OdV deve essere comunque trattata in conformità con la vigente legislazione in materia e, in particolare, in conformità al Regolamento (UE) 2016/679 (General Data Protection Regulation, cd G.D.P.R.)

Ogni informazione, segnalazione, report, relazione previsti nel Modello sono conservati dall'OdV in un apposito archivio (informatico e/o cartaceo).

4.7 Reporting dell'Organismo di Vigilanza

Al fine di garantire la sua piena autonomia e indipendenza nello svolgimento delle proprie funzioni, l'OdV relaziona direttamente al CdA e al Collegio Sindacale della Società.
L'OdV riferisce al CdA e al Collegio sindacale almeno annualmente, nella fase di approvazione del bilancio, in merito:

- agli esiti dell'attività di vigilanza espletata nel periodo di riferimento, con l'indicazione di eventuali problematiche o criticità emerse e degli interventi opportuni sul Modello;
- agli eventuali mutamenti del quadro normativo e/o significative modificazioni dell'assetto interno di Confidi Systema! e/o delle modalità di svolgimento delle attività, che richiedono aggiornamenti del Modello (tale segnalazione ha luogo qualora non si sia previamente proceduto a sottoporla al CdA al di fuori della relazione annuale);
- al resoconto delle segnalazioni ricevute, ivi incluso quanto direttamente riscontrato, in ordine a presunte violazioni delle previsioni del Modello e dei protocolli, nonché all'esito delle conseguenti verifiche effettuate;
- ai provvedimenti disciplinari ed alle sanzioni eventualmente applicate da Confidi Systema!, con riferimento alle violazioni delle previsioni del Modello e dei protocolli;
- al rendiconto delle spese sostenute;

- alle attività pianificate cui non si è potuto procedere per giustificate ragioni di tempo e risorse;
- al piano delle verifiche predisposto per l'anno successivo.

L'OdV potrà in ogni momento chiedere di essere sentito dal CdA qualora accerti fatti di particolare rilevanza, ovvero ritenga opportuno un esame o un intervento in materie inerenti il funzionamento e l'efficace attuazione del Modello.

A garanzia di un corretto ed efficace flusso informativo, l'OdV ha inoltre la possibilità, al fine di un pieno e corretto esercizio dei propri poteri, di chiedere chiarimenti o informazioni direttamente all'Amministratore Delegato.

L'OdV può, a sua volta, essere convocato in ogni momento dal CdA per riferire su particolari eventi o situazioni relative al funzionamento e al rispetto del Modello.

4.8 Flussi informativi nei confronti dell'Organismo di Vigilanza

L'Organismo di Vigilanza deve essere tempestivamente informato, mediante apposito sistema di comunicazione in merito a quegli atti, comportamenti od eventi che possono determinare una violazione del Modello o che, più in generale, sono rilevanti ai fini del d.lgs. n. 231/2001.

L'obbligo di informazione su eventuali comportamenti contrari alle disposizioni contenute nel Modello rientra nel più ampio dovere di diligenza ed obbligo di fedeltà del prestatore di lavoro.

I Destinatari delle Linee di Condotta hanno l'obbligo di segnalare all'Organismo di Vigilanza ogni violazione o sospetta violazione delle Linee di Condotta e del Modello, come di seguito meglio specificato.

L'Organismo di Vigilanza valuta tutte le segnalazioni ricevute e intraprende le conseguenti iniziative a sua ragionevole discrezione e responsabilità nell'ambito delle proprie competenze, ascoltando eventualmente l'autore della segnalazione ed il responsabile della presunta violazione. Ogni conseguente decisione sarà motivata; gli eventuali provvedimenti conseguenti potranno costituire inadempimento alle obbligazioni primarie del rapporto di lavoro e/o contrattuale, con la possibilità di irrogazione nei confronti dei responsabili di misure sanzionatorie secondo le modalità previste da leggi, accordi collettivi, contratti.

L'OdV agisce in modo da garantire gli autori delle segnalazioni contro qualsiasi forma di ritorsione, discriminazione, penalizzazione o qualsivoglia conseguenza derivante dalle stesse, assicurando loro la riservatezza circa l'identità, fatti comunque salvi gli obblighi di legge e la tutela dei diritti della Società o delle persone accusate erroneamente o in mala fede.

I flussi informativi hanno pertanto ad oggetto tutte le informazioni e tutti i documenti che devono pervenire all'OdV al fine di consentire a quest'ultimo di aumentare il livello di conoscenza della Società, di acquisire informazioni atte a valutare la rischiosità insita in taluni processi sensibili, nonché di svolgere le proprie attività di verifica e di vigilanza in merito all'efficacia e all'osservanza del Modello.

I protocolli decisionali, le Procedure e le Policy - che costituiscono parte integrante del Modello – prevedono obblighi informativi relativi ai processi e alle attività sensibili e gravanti in generale sui destinatari del Modello (es. modifiche alle attività sensibili, anomalie di processo, rilievi di audit, informazioni rilevanti).
Sono stati inoltre identificati flussi informativi originati dalle funzioni di controllo e da altre strutture della Società che, in forza delle proprie attribuzioni, svolgono attività rilevanti ai fini del D. Lgs. n. 231/01.

A titolo esemplificativo i flussi informativi includono:

- operazioni che ricadano nella attività sensibili (ad es. prospetti periodici riepilogativi sulle convenzioni stipulate con Soggetti Pubblici, informazioni relative a nuove assunzioni di personale o utilizzo di risorse finanziarie per l'acquisto di beni e servizi o altre attività di investimento, etc...);
- provvedimenti e/o notizie provenienti da organi di polizia giudiziaria o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D. Lgs. 231/01 e che possano coinvolgere Confidi Systema!;
- richieste di assistenza legale inoltrate dai dipendenti in caso di avvio di procedimento giudiziario nei loro confronti ed in relazione ai reati di cui D. Lgs. 231/01 e che possano coinvolgere Confidi Systema!;
- i documenti predisposti dalle strutture di controllo (ad esempio Internal Audit, Compliance e Antiriciclaggio, Risk Management) nell'ambito delle loro attività di verifica, dai quali possano emergere fatti, atti, eventi od omissioni con profili di criticità rispetto all'osservanza delle norme del D. Lgs. 231/01 o delle previsioni del Modello e dei protocolli di decisione;
- la pianificazione e le relazioni annuali delle attività svolte dalle funzioni di controllo;
- le contestazioni per omessa segnalazione di operazione sospetta ai sensi della normativa antiriciclaggio;
- la lettera annuale della società di revisione con evidenza delle eventuali anomalie rilevate nel processo di redazione del Bilancio Consolidato e del Bilancio d'Esercizio di Confidi Systema! e l'evidenza periodica circa il monitoraggio delle azioni correttive;
- l'informativa sull'esercizio delle deleghe e delle sub-deleghe da parte delle strutture della Società e l'aggiornamento del sistema delle procure aziendali;
- le visite, le ispezioni e gli accertamenti avviati da parte degli enti competenti (a titolo meramente esemplificativo ATS, INPS, INAIL ecc.) o da parte di Autorità di Vigilanza e, alla loro conclusione, i relativi esiti;
- la reportistica in materia di salute e sicurezza sul lavoro incluse le segnalazioni di incidenti/infortuni, anche derivanti da fattori esterni (es. rapine), che hanno comportato lesioni gravi o gravissime a dipendenti e/o a terzi;
- i procedimenti disciplinari avviati per violazioni del Modello e dei protocolli di decisione, l'applicazione di sanzioni ovvero i provvedimenti di archiviazione di tali procedimenti e le relative motivazioni;
- i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per i reati contemplati dal D.Lgs. 231/01 e che possano coinvolgere Confidi Systema!;
- i contenziosi aventi come controparte enti o soggetti pubblici (o soggetto equiparato) e, alla loro conclusione, i relativi esiti;
- le sentenze di condanna di dipendenti Confidi Systema! a seguito del compimento di reati rientranti tra quelli presupposto del D.Lgs. 231/01.

Per quanto concerne consulenti o collaboratori esterni, è contrattualmente previsto un obbligo di informativa immediata a loro carico nel caso in cui gli stessi ricevano, direttamente o indirettamente, da un dipendente di Confidi Systema! una richiesta di comportamenti che potrebbero determinare una violazione del Modello.

Nel normale svolgimento delle proprie funzioni e in ragione di considerazioni "*risk-based*", l'OdV si riserva, qualora lo ritenga opportuno, di richiedere qualsiasi informazione necessaria per l'esecuzione delle sue funzioni.

Il corretto adempimento dell'obbligo di informazione da parte del prestatore di lavoro non può dar luogo all'applicazione di sanzioni disciplinari.

Le informazioni di cui sopra possono essere segnalate all'OdV tramite una delle seguenti modalità:
Casella di posta elettronica riservata:

- Organismo di Vigilanza (odv@confidisystema.com)
Forma cartacea al seguente indirizzo:
Confidi Systema! - Organismo di Vigilanza 231/01

All'attenzione del Presidente dell'Organismo di Vigilanza
via Lepetit, 8
20124 Milano (MI)

5. LA DIFFUSIONE DEL MODELLO E LA FORMAZIONE

Al fine di garantire la reale efficacia del Modello, i suoi contenuti devono essere portati a conoscenza di tutti i Destinatari i quali devono, altresì, avere cognizione che, dal momento dell'adozione del Modello, in caso di qualsivoglia violazione delle sue regole, verrà irrogata una delle sanzioni previste.

Pertanto Confidi Systema!, tramite il suo OdV, si occuperà della diffusione del presente Modello attraverso la pubblicazione del testo integrale, o di un suo estratto, attraverso i canali di comunicazione aziendale (sito internet, eventuale Intranet, all'affissione in bacheca in ciascuna sede) e provvederà altresì al suo aggiornamento periodico.

5.1 La formazione del personale

Al fine di perseguire un'idonea sensibilizzazione in materia di responsabilità amministrativa degli enti, Confidi Systema!, sotto il controllo dell'OdV, si occuperà della formazione nel seguente modo.

5.2 Personale Dirigente e con funzioni di rappresentanza (c.d. Soggetti apicali)

La formazione del personale Dirigente e con funzioni di rappresentanza verrà effettuata, su iniziativa dell'OdV, per mezzo dei seguenti strumenti:

- distribuzione di una copia del Modello, seguita da una dichiarazione sottoscritta dal soggetto per presa visione e impegno ad osservarne le prescrizioni in esso contenute;
- corso di formazione iniziale in merito ai contenuti del Decreto;
- aggiornamento annuale, concernente modificazioni e/o integrazioni della normativa;
- e-mail periodiche di aggiornamento.

Per i nuovi assunti:

- distribuzione di una copia del Modello, seguita da una dichiarazione sottoscritta dal soggetto per presa visione e impegno ad osservarne le prescrizioni in esso contenute;
- corso di formazione iniziale in merito ai contenuti del Decreto, all'assunzione.

5.3 Altro personale

La formazione di altro personale (inteso quale personale non dirigente e senza funzioni di rappresentanza) verrà effettuata, su iniziativa dell'OdV, per mezzo dei seguenti strumenti:

- distribuzione di una copia del Modello, seguita da una dichiarazione sottoscritta dal soggetto per presa visione e impegno ad osservarne le prescrizioni in esso contenute;
- e-mail di aggiornamento periodiche.

Per i nuovi assunti:

- distribuzione di una copia del Modello, seguita da una dichiarazione sottoscritta dal soggetto per presa visione e impegno ad osservarne le prescrizioni in esso contenute.

5.4 L'informativa ai soggetti esterni alla Società

Confidi Systema! si dovrà attivare per la distribuzione del Modello o di un estratto dello stesso anche nei confronti di partners commerciali, collaboratori, consulenti, clienti, fornitori e soggetti esterni che, operano a vario titolo con la Società o che compiono atti a vantaggio o nell'interesse di essa.

Tali soggetti sono tenuti a sottoscrivere una dichiarazione di presa visione del presente Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01 che attesti il ricevimento della copia e l'impegno a rispettarne tutte le disposizioni.

6. IL SISTEMA SANZIONATORIO

Ferme restando le sanzioni previste da provvedimenti normativi per violazioni di disposizioni in essi contenute, Confidi Systema! stabilisce che le sanzioni che adotterà nei confronti dei Destinatari che abbiano tenuto comportamenti contrari alle indicazioni Modello, saranno irrogate secondo il criterio di proporzionalità in base alla gravità ed intenzionalità dell'infrazione commessa, tenendo anche conto dell'eventuale reiterazione degli inadempimenti e/o violazioni commesse.

Per dipendenti e/o dirigenti il rispetto del Modello è parte integrante delle condizioni che regolano i rapporti di lavoro nella Società e ogni violazione al presente Modello comporterà l'adozione di provvedimenti disciplinari proporzionati alla gravità o recidività della mancanza o al grado della colpa, nel rispetto delle disposizioni contenute nei contratti di lavoro applicabili (art. 7 della Legge 20 maggio 1970, n. 300) e da quanto disposto dal D. Lgs. 8 giugno 2001, n. 231.

Gli artt. 6 e 7 di tale provvedimento prevedono, infatti, che gli enti siano esonerati dalla responsabilità amministrativa - penale, qualora abbiano adottato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire i reati del tipo di quello verificatosi e correlato ad un sistema di sanzioni "disciplinari" da adottare nel caso di inosservanza delle regole contenute nel Decreto stesso.

Per quanto riguarda gli altri Destinatari del Codice, la violazione delle disposizioni ivi incluse comporta l'adozione di provvedimenti proporzionati alla gravità o recidività della mancanza o al grado della colpa, sino alla risoluzione dei contratti in essere con gli stessi per giusta causa ovvero per inadempimento dei soggetti pocanzi indicati.

Pertanto, i comportamenti non conformi alle disposizioni del presente Modello comporteranno, indipendentemente ed oltre gli eventuali procedimenti penali a carico del/degli autore/i della violazione, l'applicazione di sanzioni disciplinari ai sensi di quanto sopra rappresentato.

7. PROTOCOLLI

SELEZIONE E APPROVVIGIONAMENTO FORNITORI

Descrizione processo
Il processo di acquisizione di beni e servizi si articola nelle seguenti fasi:

- emissione della Richiesta di Acquisto;
- scelta del fornitore e formalizzazione contrattuale;
- gestione dei rapporti col fornitore;
- rilascio benestare, contabilizzazione e pagamento fatture.

Attività di Controllo
Il sistema di controllo si basa sugli elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti, a garanzia della trasparenza delle scelte effettuate e della valutazione complessiva delle forniture.
In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

1) Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
   - richiesta della fornitura;
   - effettuazione dell'acquisto;
   - certificazione dell'esecuzione dei servizi/consegna dei beni;
   - effettuazione del pagamento.

2) Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva:
   - comparazione delle offerte (sulla base di criteri oggettivi e documentabili ed in un'ottica volta ad assicurare a Confidi Systema! la migliore configurazione possibile di costo, qualità e tempo).

3) Verifica preventiva dei contratti di fornitura:
   - Confidi Systema! richiede al fornitore una bozza del contratto che sarà oggetto di verifica del Responsabile del settore di riferimento e, ove ritenuto necessario, del Responsabile dell'Ufficio Legale o al Responsabile Compliance;
   - al fine di garantire la liceità e la piena pertinenza di ogni rapporto di affari che Confidi Systema! intrattiene con i propri fornitori, si richiede al fornitore una dichiarazione di presa visione del Codice Etico e di impegno ad attenersi ai principi e alle regole che compongono il Modello di Organizzazione, Gestione e Controllo (ex D.Lgs. 231/01) con l'espresso avvertimento che a fronte di eventuali violazioni verranno adottate delle sanzioni, quali la risoluzione del contratto stesso;
   - nel caso non sia possibile inserire la suddetta clausola negli accordi tra società e soggetto terzo, Confidi Systema! invia mediante posta elettronica certificata o lettera raccomandata A.R o a mani., un'informativa finalizzata a notificare alla controparte l'esistenza di un Codice Etico aziendale, che fa parte di un Modello di Organizzazione, Gestione e Controllo (ex D.Lgs. 231/01) adottato da Confidi Systema!.

Confidi Systema! si accerta di ricevere, come risposta all'informativa, una specifica dichiarazione di avvenuta presa di conoscenza.

4) Esistenza di livelli di approvazione per le richieste di acquisto e per la certificazione della fornitura/erogazione.
5) Esistenza di livelli autorizzativi (in coerenza con il sistema di procure aziendale) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.

6) Tenuta a manutenzione dell'albo dei fornitori tra cui dovrà preferibilmente essere selezionato il fornitore.
7) Compilazione scheda di valutazione del fornitore a cura del Responsabile dell'area.
8) Tracciabilità delle singole fasi del processo, per consentire la ricostruzione delle responsabilità, delle motivazioni delle scelte e delle fonti informative.

Indicazioni comportamentali generali

È fatto obbligo di:

- segnalare tempestivamente alle strutture/aree competenti qualsiasi comportamento in contrasto con quanto prescritto dal Modello: tale obbligo grava su tutti i dipendenti della Società, che vengano in qualsiasi forma a conoscenza, nonché sui fornitori, che li subiscano; qualora i fornitori non adempiano a tale obbligo, saranno estromessi dall'elenco dei fornitori e dal singolo affare.

È fatto divieto di:

- esercitare violenze, minacce, pressioni, attività ingannatorie o comunque indebite sollecitazioni nei confronti delle parti contraenti, anche su induzione da parte delle medesime, finalizzate al conseguimento di illeciti vantaggi per l'ente nel cui interesse questi agiscono;
- richiedere o accettare elargizioni o promesse di denaro o di altre utilità, compresi omaggi o regali;
- utilizzare fornitori scelti principalmente in base a criteri di amicizia, parentela o altra cointeressenza, e comunque tali da inficiare la validità in termini di prezzo e/o qualità, o che appaiano meramente strumentali alla realizzazione di una delle condotte illecite indicate nel D.Lgs. 231/01;
- negoziare condizioni contrattuali occulte, che non risultano da idonea documentazione conservata unitamente a quella relativa all'acquisto.

In particolare, nelle seguenti attività è fatto divieto di tenere comportamenti che:

- Richiesta della fornitura:
  - consentano di non espletare un'adeguata attività selettiva fra i diversi offerenti e di obiettiva comparazione delle offerte;
  - consentano di privilegiare fornitori segnalati o "graditi" a soggetti pubblici in assenza dei criteri tecnico-economici per la selezione dei potenziali candidati (Qualificazione e inserimento in un Albo Fornitori).
- Effettuazione dell'acquisto:
  - consentano a soggetti non autorizzati di procedere alla stipulazione dei contratti ed all'approvazione delle relative varianti/integrazioni.
- Certificazione dell'esecuzione dei servizi/consegna dei beni
  - consentano l'emissione di fatture a fronte di forniture in tutto o in parte inesistenti o la creazione di fondi patrimoniali a fronte di forniture contrattualizzate a prezzi non congrui o non corrispondenti a quanto pattuito in sede di definizione contrattuale;
  - consentano di effettuare pagamenti che non trovino adeguata giustificazione in relazione alla fornitura oggetto del contratto.
- Effettuazione del pagamento
  - non consentano di liquidare gli importi dovuti in modo trasparente, documentabile e ricostruibile ex post. In particolare, che non consentano la verifica circa la corrispondenza fra il soggetto beneficiario del pagamento ed il fornitore.

CONSULENZE E PRESTAZIONI PROFESSIONALI

Descrizione processo

Il processo riguarda l'assegnazione di incarichi di consulenza e prestazioni professionali a soggetti terzi e pertanto si configura, pur nella specificità dell'oggetto contrattuale, come un processo d'acquisizione, articolato nelle seguenti fasi:

- emissione della Richiesta di Consulenza/Prestazione Professionale;
- scelta della fonte d'acquisto e formalizzazione del contratto;
- gestione operativa del contratto;
- rilascio benestare, contabilizzazione e pagamento fatture.

Attività di Controllo

Il sistema di controllo si basa sui due elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo, della tracciabilità degli atti, a garanzia della trasparenza delle scelte effettuate e del servizio ricevuto.

In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di attori diversi operanti nelle seguenti fasi/attività del processo:
  - richiesta della consulenza;
  - autorizzazione;
  - definizione contrattuale;
  - certificazione dell'esecuzione dei servizi (rilascio benestare);
  - effettuazione del pagamento.
- Esistenza di requisiti professionali, economici ed organizzativi a garanzia degli standard qualitativi richiesti.
- Espletamento di adeguata attività selettiva fra diversi offerenti e di obiettiva comparazione delle offerte (sulla base di criteri oggettivi e documentabili); in assenza di tale attività selettiva evidenziazione formale delle ragioni della deroga ed esecuzione da parte del responsabile di una valutazione sulla congruità del compenso pattuito (rispetto agli standard di mercato).
- Utilizzo di idonei dispositivi contrattuali adeguatamente formalizzati.
- Per consulenze svolte da soggetti terzi incaricati di rappresentare la Società deve essere prevista una specifica clausola che li vincoli all'osservanza dei principi etico-comportamentali adottati dalla stessa.
- Esistenza di livelli di approvazione per le richieste di consulenza.
- Validazione del servizio reso.
- Esistenza di livelli autorizzativi (in coerenza con il sistema di procure/poteri aziendali) per la stipulazione dei contratti e l'approvazione delle relative varianti/integrazioni.
- Tracciabilità delle singole fasi del processo (documentazione a supporto, livello di formalizzazione e modalità/tempistiche di archiviazione).

Sono escluse: le consulenze e le prestazioni professionali di modesto importo.

Indicazioni comportamentali

In tutte le fasi del processo, ed in particolare nelle seguenti attività è fatto divieto di tenere comportamenti che:

- Richiesta della consulenza
  - consentano l'inoltro della richiesta di conferimento dell'incarico a consulenti esterni per lo svolgimento di attività che possono essere svolte da risorse interne alla Società.

- Autorizzazione alla consulenza
  - consentano l'affidamento dell'incarico in assenza di previa selezione fra una rosa di almeno due potenziali consulenti, ad eccezione delle forniture per le quali si richiede una particolare tecnicalità e previa motivazione espressa;
  - consentano l'assegnazione dell'incarico a ex dipendenti della Pubblica Amministrazione o dell'Unione Europea che abbiano partecipato personalmente ed attivamente a una trattativa d'affari o abbiano avallato le richieste effettuate alla Pubblica Amministrazione dalla Società o da società controllate, collegate della medesima o sottoposte a comune controllo con la medesima;
  - consentano l'assegnazione dell'incarico a persone o società "vicine" o "gradite" a soggetti pubblici o privati con i quali la Società ha rapporti commerciali e/o interessi in assenza dei necessari requisiti di qualità e convenienza dell'operazione;
  - consentano la scelta di consulenti che non garantiscano la migliore combinazione in termini di qualità del servizio, prezzo, tempi di consegna, congruità del corrispettivo pattuito ecc.;
  - consentano l'autorizzazione al conferimento dell'incarico al consulente da parte di soggetti a ciò non autorizzati.
- Definizione contrattuale
  - consentano la mancata tracciabilità del conferimento formale dell'incarico;
  - non garantiscano l'apposizione di specifica informativa sulle norme comportamentali adottate dalla Società con riferimento al Decreto e sulle conseguenze che possono avere, con riguardo ai rapporti contrattuali, comportamenti contrari alle previsioni del Codice Etico ed alla normativa vigente.
- Certificazione dell'esecuzione dei lavori (rilascio benestare)
  - consentano l'emissione di fatture o la creazione di fondi patrimoniali a fronte di operazioni in tutto o in parte inesistenti o a fronte di operazioni contrattualizzate a prezzi superiori di quelli di mercato o comunque non congrui o corrispondenti a quanto pattuito in sede di definizione contrattuale;
  - consentano di effettuare pagamenti e riconoscere rimborsi spese in favore di consulenti, che non trovino adeguata giustificazione in relazione al tipo di incarico svolto, che non siano supportate da giustificativi fiscalmente validi e che non siano esposte in fattura o in parcella.
- Effettuazione del pagamento
  - non consentano di liquidare i compensi in modo trasparente, documentabile e ricostruibile ex post. In particolare, che non consentano la verifica circa la corrispondenza fra il soggetto beneficiario del pagamento ed il consulente che ha effettivamente erogato il servizio oggetto dell'incarico conferito.

UTILIZZO DEGLI STRUMENTI INFORMATICI

Descrizione processo
Il processo di "Utilizzo degli Strumenti Informatici" si articola in attività volte alla gestione, alla manutenzione e/o all'utilizzo di Sistemi Informativi, inclusi i sistemi di terzi e/o forniti da terzi.

Il processo si articola nelle seguenti fasi:
- identificazione del fabbisogno di accesso al/i sistema/i;
- definizione profili di accesso e attivazione al/i sistema/i;
- manutenzione di/del sistema/i (tra cui: attività di controllo, verifica eccezioni/anomalie).

L'infrastruttura tecnologica e i sistemi informatici rappresentano una risorsa fondamentale e strategica per la Società; l'utilizzo di strumenti e tecnologie informatiche è diffuso e trasversale all'interno della Società: il personale appartenente alle diverse aree aziendali utilizza sistematicamente gli strumenti informatici messi a disposizione per lo svolgimento delle attività di propria competenza, in qualità di utente interno, nell'ambito ad esempio della gestione dei processi di amministrazione, contabilità e controllo di gestione.
I profili di accesso al sistema informatico sono puntualmente identificati dalle competenti strutture in coordinamento con le funzioni/aree interessate, in modo che sia garantita la separatezza delle funzioni e la coerenza dei livelli autorizzativi.
L'uso di credenziali di accesso a sistemi, applicazioni e/o banche dati di terze parti deve essere formalmente autorizzato dalla Direzione Generale così come le variazioni al contenuto dei profili (estensioni delle autorizzazioni) che sono eseguite esclusivamente dall'amministratore di sistema, su richiesta delle funzioni/aree interessate. La funzione/area richiedente deve comunque garantire che le abilitazioni informatiche richieste corrispondano alle mansioni lavorative coperte.
Resta inteso che i diritti di accesso alle risorse di rete (cartelle condivise, stampanti, ecc) sono definiti dalla Direzione Generale e configurati sul server direttamente dal responsabile EDP In particolare i diritti di accesso alla rete richiedono la definizione di diritti specifici per singoli utenti, che devono essere documentate, ridotte in termini numerici e sempre autorizzate dalla Direzione Generale.
Le attività di gestione ed utilizzo dei sistemi informativi della Società sono soggette a una costante attività di controllo che si esplica sia attraverso l'utilizzo di adeguate misure per la protezione delle informazioni, salvaguardandone la riservatezza, l'integrità e la disponibilità con particolare riferimento al trattamento dei dati personali, sia tramite l'adozione, per l'insieme dei processi aziendali, di specifiche soluzioni di continuità operativa di tipo tecnologico, organizzativo e infrastrutturale che assicurino la predetta continuità anche a fronte di situazioni di emergenza.
Tra i servizi aziendali di base accessibili ai dipendenti e collaboratori dotati di postazioni di lavoro personali vi sono in particolare la posta elettronica e la navigazione in internet, il cui utilizzo è regolato da specifiche procedure e misure di sicurezza.
Qualora sia previsto il coinvolgimento di soggetti terzi (a titolo esemplificativo, fornitori, consulenti e professionisti) nelle attività a rischio-reato di cui alla presente Parte Speciale, il sistema dei controlli e i principi di comportamento ivi contenuti si applicano anche a presidio delle attività poste in essere dagli stessi.

Attività di Controllo
Il sistema di controllo per la prevenzione dei reati di criminalità informatica si basa, nel rispetto della normativa applicabile, sugli elementi qualificanti della tracciabilità, della formalizzata separazione di ruolo nelle fasi chiave del processo, oltre che sul rispetto del Codice Etico e delle Linee di Condotta e del complesso della normativa interna (Regolamenti, Circolari, Manuali, Procedure aziendali) vigente.
In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- **Separazione** dei ruoli che intervengono nelle attività di gestione e accesso ai Sistemi Informativi.
    - **Tracciabilità** degli accessi degli amministratori di sistema e delle attività modificative svolte sui sistemi informatici. In particolare:
        - tutti i documenti sono salvati e archiviati in apposite cartelle elettroniche, denominate per argomento e data, presenti sul server della Società;

- le operazioni eseguite dall'amministratore di sistema dai fornitori esterni sono tracciate secondo quanto previsto dal Provvedimento del Garante del 27 novembre 2007 "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema";
- in generale, al fine di consentire la ricostruzione delle responsabilità e delle motivazioni delle scelte effettuate, la funzione/area di volta in volta interessata è responsabile dell'archiviazione e della conservazione di tutta la documentazione prodotta anche in via telematica o elettronica;
- il processo decisionale, con riferimento all'attività di gestione e utilizzo di sistemi informatici, è garantito dalla completa tracciabilità a sistema;
- è garantita la completa tracciabilità di tutti gli eventi e le attività effettuate (tra le quali gli accessi alle informazioni, le operazioni correttive effettuate tramite sistema, ad esempio rettifiche contabili, variazioni dei profili utente, ecc.), con particolare riguardo all'operato di utenze con privilegi speciali.

- **Raccolta, analisi e gestione di segnalazioni** a fronte di eccezioni/anomalie rilevate.

Indicazioni comportamentali

Per la prevenzione dei crimini informatici, i dipendenti e i collaboratori della Società devono adottare comportamenti conformi, oltre che al Codice Etico e alle Linee di Condotta, anche a tutte le direttive e norme di comportamento contenute nelle politiche e regolamenti in vigore per assicurare i livelli richiesti di sicurezza. In particolare, non devono essere adottati comportamenti a rischio di reato e non conformi alle suddette norme nell'ambito delle attività svolte a supporto dei principali processi aziendali, nonché, nell'utilizzo degli strumenti informatici che consentono l'accesso ai siti e di pubblica utilità, quando l'utilizzo illecito o non conforme di tali strumenti può provocare il danneggiamento di informazioni pubblicate, procurando un profitto ovvero un vantaggio competitivo o di immagine alla Società.

Il Personale è responsabile del corretto utilizzo degli strumenti informatici a lui assegnati (ad esempio, personal computer fissi o portatili), che devono essere utilizzate in conformità con le normative interne. Tali strumenti devono essere conservati in modo appropriato e la Società deve essere tempestivamente informata di eventuali furti o danneggiamenti.

Il Personale è tenuto alla segnalazione alle competenti strutture dell'Area EDP di eventuali incidenti di sicurezza, anche concernenti attacchi al sistema informatico da parte di hacker esterni).

<u>È in particolare fatto divieto di</u>:

- introdursi abusivamente, direttamente o per interposta persona, in un sistema informatico o telematico protetto da misure di sicurezza contro la volontà del titolare del diritto all'accesso anche al fine di acquisire informazioni riservate;
- accedere al sistema informatico o telematico, o a parti di esso, ovvero a banche dati della Società o a parti di esse, non possedendo le credenziali d'accesso o mediante l'utilizzo delle credenziali di altri colleghi abilitati;
- intercettare fraudolentemente e/o diffondere, mediante qualsiasi mezzo di informazione al pubblico, comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi;
- utilizzare dispositivi tecnici o strumenti software non autorizzati (virus, worm, trojan, spyware, dialer, keylogger, rootkit, ecc.) atti ad impedire o interrompere le comunicazioni relative ad un sistema informatico o telematico o intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare, sopprimere informazioni, dati o programmi informatici altrui o anche solo mettere in pericolo l'integrità e la disponibilità di informazioni, dati o programmi utilizzati dallo Stato o da altro Ente pubblico o ad essi pertinenti o comunque di pubblica utilità;
- introdurre o trasmettere dati, informazioni o programmi al fine di distruggere, danneggiare, rendere in tutto o in parte inservibili, ostacolare il funzionamento dei sistemi informatici o telematici di pubblica utilità;

- detenere, procurarsi, riprodurre o diffondere abusivamente codici d'accesso o comunque mezzi idonei all'accesso di un sistema protetto da misure di sicurezza;
- procurare, riprodurre, diffondere, comunicare, mettere a disposizione di altri, apparecchiature, dispositivi o programmi al fine di danneggiare illecitamente un sistema o i dati e i programmi ad esso pertinenti ovvero favorirne l'interruzione o l'alterazione del suo funzionamento;
- alterare, mediante l'utilizzo di firma elettronica altrui o comunque in qualsiasi modo, documenti informatici;
- produrre e trasmettere documenti in formato elettronico con dati falsi e/o alterati;
- porre in essere, collaborare o dare causa alla realizzazione di comportamenti tali che, presi individualmente o collettivamente, integrino, direttamente o indirettamente, le fattispecie di reato contemplate nel Decreto, nonché atti idonei diretti in modo non equivoco a realizzarle;
- porre in essere comportamenti che, sebbene risultino tali da non costituire di per sé fattispecie di reato, possano potenzialmente diventarlo.

I Destinatari sono inoltre tenuti a osservare le previsioni legislative esistenti in materia e i principi contenuti nel Codice Etico, nel Documento Programmatico sulla Sicurezza dei dati per la gestione sicurezza fisica e logica del backup (DPS) e nel Piano di Continuità Operativa e del Disaster Recovery (BC&DR).

ADEMPIMENTI ANTIRICICLAGGIO

Descrizione processo
La Società effettua un'accurata attività di formazione e addestramento per tutte le aree aziendali. Per garantire continuità e sistematicità all'attività di qualificazione del personale, l'attività di formazione in materia di antiriciclaggio è incentrata sulla partecipazione del personale sia a corsi esterni e interni, sia a aggiornamenti periodici sull'evoluzione della normativa.

Attività di Controllo
Il sistema di controllo si basa sugli elementi qualificanti della formalizzata separazione di ruolo nelle fasi chiave del processo e della tracciabilità degli atti.
In particolare, gli elementi specifici di controllo sono di seguito rappresentati.

- Esistenza di direttive sulle modalità di condotta operativa da adottare in attuazione della normativa antiriciclaggio.
- Istituzione di una Funzione Antiriciclaggio.
- Formalizzazione di una politica e di una procedura antiriciclaggio.
- Formalizzazione degli eventuali rapporti con soggetti esterni (consulenti legali, terzi rappresentanti o altro) incaricati di svolgere attività antiriciclaggio a favore della Società, prevedendo, tra l'altro, nei contratti, l'inserimento di una specifica clausola che li vincoli al rispetto dei principi etico-comportamentali adottati dalla Società.
- Rendicontazione in merito agli adempimenti antiriciclaggio posti in essere ed alle relative risultanze e tracciabilità degli atti e delle fonti documentali che ne stanno alla base.

Indicazioni comportamentali
È fatto divieto di adottare comportamenti contrari al Codice Etico e alle Linee di Condotta in tutte le fasi del processo ed in particolare nelle seguenti attività:

- in sede di gestione ed implementazione degli adempimenti antiriciclaggio a cui la Società è tenuta;
- nel corso delle fasi degli adempimenti antiriciclaggio anche a mezzo di soggetti terzi di cui la Società eventualmente si avvale;
- in sede di ispezioni e verifiche da parte della Autorità competenti.

Nello specifico:

- ai sensi della normativa vigente, qualora non vi sia la possibilità di adempiere agli obblighi di identificazione e verifica del cliente o del titolare effettivo o dell'eventuale esecutore, ovvero di ottenere le informazioni sullo scopo e la natura del rapporto, quindi laddove il cliente rifiuti di fornire al soggetto che entra in contatto con il cliente le informazioni e/o i documenti richiesti ai fini del corretto assolvimento degli obblighi di adeguata verifica oppure la Società, non sia in grado di verificare la veridicità e/o l'attendibilità dei dati/documenti raccolti la Società deve astenersi dall'instaurare il rapporto continuativo;
- sono dettagliati nell'ambito di politiche, regolamenti/norme operative interne le regole comportamentali ad integrazione e maggiore specificazione della normativa esterna e dei principi sanciti dal Modello in materia di contrasto al riciclaggio e finanziamento del terrorismo;
- in caso di richiesta di chiarimenti da parte delle funzioni/aree gerarchicamente sovraordinate, i responsabili della funzione/area forniscono le informazioni in modo tempestivo;
- devono essere assicurate lo sviluppo e la gestione operativa delle applicazioni utilizzate nelle attività di contrasto finanziario al terrorismo/riciclaggio;
- deve essere verificato e garantito l'aggiornamento / manutenzione / diffusione delle liste interne di soggetti/ Paesi/ merci interessati da provvedimenti restrittivi emanati da UE, OFAC, BI-UIF;
- nel caso di valutazione di clientela ovvero di operazioni che interessino più strutture operative, le stesse devono collaborare tra loro e, ove consentito dalla normativa vigente, scambiare le informazioni finalizzate alla completa ed adeguata conoscenza del cliente e delle sue abitudini operative;

- è necessario assicurare con continuità e sistematicità la formazione e l'addestramento del personale sulla normativa antiriciclaggio e sulle finalità dalle stesse perseguite;
- devono essere diffusi a tutti i collaboratori, indipendentemente dalle mansioni in concreto svolte, la normativa di riferimento ed i relativi aggiornamenti;
- tutti i Destinatari del Modello, senza distinzioni di rapporto giuridico in base al quale sono legati alla Società, devono partecipare fattivamente al processo di analisi della clientela e della relativa attività per l'individuazione e la segnalazione di operazioni sospette; in tale ambito, ciascun collaboratore dovrà fare riferimento al Responsabile della funzione/area aziendale di appartenenza, comunicando allo stesso per iscritto ogni operazione, comportamento, anomalia, per qualsivoglia circostanza conosciuta a ragione delle funzioni esercitate, reputata suscettibile di valutazione ai fini di un eventuale avvio dell'iter di segnalazione.

Con specifico riferimento al reato di autoriciclaggio, rilevano inoltre come attività a rischio-reato gli ambiti aziendali nei quali potrebbero potenzialmente essere generati illecitamente denaro, beni o altre utilità (successivamente impiegabili, sostituibili, trasferibili in attività economiche, finanziarie, imprenditoriali o speculative). A titolo esemplificativo, possono essere individuate le seguenti attività a rischio-reato: Stipula e gestione dei rapporti contrattuali con la clientela e le controparti (partner commerciali), Gestione degli approvvigionamenti, degli incarichi professionali e delle consulenze, Operazioni di rilevazione, registrazione e rappresentazione dell'attività di impresa nelle scritture contabili, nei bilanci, nelle relazioni sulla gestione e in altri documenti di impresa e di gestione degli aspetti fiscali.

I principi di controllo e di comportamento implementati con riferimento a dette attività sono pertanto considerati validi presidi anche ai fini della prevenzione del reato di autoriciclaggio.

In generale, comunque, ove non sia chiara la provenienza di denaro, beni o altre utilità oggetto di attività e/o operazioni svolte nell'ambito dell'operatività aziendale, nonché in tutti i casi in cui si riscontrino elementi tali da farne sospettare una provenienza delittuosa, i Destinatari coinvolti sono tenuti a sospendere immediatamente le attività e/o operazioni interessate, comunicando e rappresentando il fatto ai propri responsabili e a eventuali altri soggetti/strutture/aree competenti, affinché siano posti in essere gli approfondimenti e accertamenti necessari.

SPESE DI RAPPRESENTANZA

Descrizione processo
Il processo concerne il sostenimento di spese per la cessione gratuita di beni e servizi a favore di terzi non dipendenti, con lo scopo di offrire un'immagine positiva della Società e dell'attività.

Il processo si articola nelle seguenti fasi:
- sostenimento della spesa;
- autorizzazione al rimborso;
- rimborso.

Attività di Controllo
Il sistema di controllo si basa sugli elementi qualificanti della individuazione dei soggetti abilitati (a sostenere e ad autorizzare le spese) e sulla tracciabilità degli atti.
In particolare, gli elementi specifici di controllo sono di seguito rappresentati:
- Definizione delle categorie di spesa effettuabili;
- Identificazione dei soggetti aziendali abilitati a sostenere le spese;
- Esistenza di specifici range economici, con espressa indicazione degli importi entro i quali la spesa è da considerarsi di modico valore;
- Esistenza di livelli di autorizzazione per il rimborso delle spese effettuate;
- Esistenza di registrazione, presso il soggetto aziendale abilitato, delle spese sostenute sia a favore dei dipendenti della Pubblica Amministrazione sia dei privati.
- Esistenza, presso i soggetti coinvolti, di evidenza documentale delle singole fasi del processo.

Indicazioni comportamentali
In tutte le fasi del processo, ed in particolare nelle seguenti attività, <u>è fatto divieto di tenere comportamenti che:</u>
- Sostenimento della spesa:
  - consentano l'indicazione di voci di spesa rientranti fra quelle appartenenti alle categorie autorizzate, ma non corrispondenti a quelle effettivamente sostenute;
  - permettano il sostenimento della spesa da parte di soggetti a ciò non abilitati.
- Autorizzazione al rimborso:
  - consentano l'autorizzazione al rimborso della spesa da parte di soggetti a ciò non autorizzati;
  - consentano la registrazione di spese sostenute a favore di soggetti diversi dagli effettivi beneficiari.
- Rimborso
  - consentano il rimborso di spese non sostenute in tutto o in parte;
  - consentano il rimborso di spese non sorrette da giustificativi fiscalmente validi.

WHISTLEBLOWING

Descrizione processo

Il processo concerne le regole sui sistemi interni di segnalazione delle Violazioni (c.d. Whistleblowing) che dettano la disciplina volta a incoraggiare i dipendenti a segnalare fatti o comportamenti che possano costituire una violazione delle norme disciplinanti l'attività della Società nonché ogni altra condotta irregolare di cui vengano a conoscenza.
Il dipendente che venga a conoscenza di una violazione, tentativo o sospetto di violazione del Modello, può attivare il presente protocollo.

Per Violazione si intende qualsiasi azione od omissione, avvenuta nello svolgimento dell'attività lavorativa o che abbia un impatto sulla stessa o che possa arrecare danno o pregiudizio alla Società e/o ai suoi dipendenti e collaboratori e che:

- sia illecita, scorretta o immorale;
- violi le disposizioni normative e regolamentari;
- non sia conforme alle normative interne ivi compreso il Codice Etico ed il MOG 231.

Rientrano nell'ambito di applicazione del Whistleblowing le seguenti tipologie di segnalazioni:

- ogni violazione delle regole e/o procedure interne della Società quali, ad esempio, il Codice Etico;
- ogni condotta che dia luogo a conflitti di interesse, adottata senza aver osservato il pieno rispetto delle regole e procedure di controllo previste per tali situazioni;
- ogni condotta che possa dar luogo a illeciti penali, quali ad esempio truffa, appropriazione indebita, furto, corruzione, riciclaggio, frode, abuso di informazioni privilegiate, trattamento illecito dei dati personali, false comunicazioni all'Autorità, accesso abusivo al sistema informatico.

È assicurata la riservatezza circa l'identità del segnalante.

La responsabilità dei sistemi interni di segnalazione viene attribuita all'OdV che assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti.

L'OdV svolge i seguenti compiti:

- ricezione delle segnalazioni, garantendo al segnalante la massima riservatezza;
- effettuazione del primo esame;
- attivazione degli accertamenti;
- acquisizione degli esiti;
- supporto nella predisposizione delle informative periodiche.

Il processo si articola nelle seguenti fasi:

- segnalazione;
- analisi preliminare;
- indagine;
- gestione degli esiti;
- *escalation*;
- comunicazione finale a segnalante e segnalato ed archiviazione.

Nel dettaglio:

- segnalazione:
  - qualora un soggetto abbia il sospetto che si sia verificata o che si possa verificare una violazione, procede alla trasmissione della segnalazione inviando una mail all'indirizzo whistleblowing.cs@gmail.com;

- la segnalazione è indirizzata al responsabile il quale:
    - provvede a dare avvio alle fasi attuative del processo e ad inviare al segnalante la comunicazione per presa in carico della segnalazione;
    - registra la segnalazione ricevuta, classificandone la tipologia.

- analisi preliminare:
- il responsabile:
    - effettua una verifica formale in merito alla presenza di dati ed informazioni utili e rilevanti;
    - svolge una prima valutazione della fondatezza delle circostanze rappresentate nella segnalazione per l'avvio di ulteriori approfondimenti.

- indagine:
- l'area incaricata procede ad effettuare la valutazione della segnalazione richiedendo (solo con l'autorizzazione del responsabile che ha l'obbligo di garantire la riservatezza) chiarimenti al Segnalante;
- l'area incaricata procede inoltre con:
    - l'esecuzione degli esiti finali della valutazione;
    - la formalizzazione delle risultanze e dell'eventuale necessità di seguito, inoltrando la relazione al Responsabile.

- gestione degli esiti:
- ingaggiare l'area Risorse Umane per l'avvio di eventuali procedimenti disciplinari;
- coinvolgere la funzione Compliance e l'OdV per eventuali profili di rischio correlati alla commissione di illeciti;
- comunicare l'esito alle funzioni aziendali, concordando eventuali provvedimenti per la rimozione delle debolezze del processo aziendale impattato.

- *escalation*:
- concluse le indagini, il responsabile comunica i risultati degli approfondimenti e delle verifiche relative alla segnalazione qualora ritenuta rilevante, inclusa l'adozione (o la mancata adozione) di provvedimenti disciplinari ai soggetti apicali interessati:
    - Organismo di Vigilanza;
    - Collegio Sindacale;
    - Consiglio di Amministrazione;
    - Funzione di Internal Audit;
    - Responsabili delle strutture aziendali eventualmente interessate dai contenuti della Segnalazione.

- Comunicazione finale e archiviazione:
- il soggetto segnalante e il soggetto segnalato sono informati sugli sviluppi del procedimento.

Indicazioni comportamentali

In tutte le fasi del processo, ed in particolare nelle seguenti attività è fatto divieto di tenere comportamenti che:
- Divulgare il nome del soggetto segnalante

Si segnala che, in casi ritenuti particolarmente gravi, in alternativa al protocollo di segnalazione come qui rappresentato, i dipendenti o i collaboratori di un soggetto vigilato da Banca d'Italia possono utilizzare lo strumento di *whistleblowing* creato da Banca d'Italia per segnalare possibili violazioni della normativa o anomalie gestionali riscontrate ("Segnalazioni Whistleblowing").Per presentare una segnalazione whistleblowing è disponibile sul sito internet della Vigilanza (https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/schema-modulo-segnalazioni-WB.pdf) il modulo "Segnalazione Whistleblowing" da inviare alla Banca d'Italia:

- via posta elettronica alla casella whistleblowing-vigilanza@bancaditalia.it; oppure
- via posta ordinaria, all'indirizzo Banca d'Italia, via Nazionale, n. 91 - 00184 Roma, all'attenzione del Dipartimento Vigilanza bancaria e finanziaria - Servizio CRE - Divisione SRE (la busta deve recare la dicitura "riservato").

Anche coloro che non sono dipendenti o collaboratori di soggetti vigilati dalla Banca d'Italia possono presentare segnalazioni su possibili violazioni della normativa o presunte anomalie gestionali riscontrate presso gli intermediari ("Segnalazioni Aziendali") attraverso il modulo "Segnalazione aziendale" disponibile sul sito della vigilanza al seguente percorso: https://www.bancaditalia.it/compiti/vigilanza/whistleblowing/Modulo-segnalazioni-aziendali.pdf.
Il modulo può essere inviato alla Banca d'Italia:

- via posta elettronica alla casella segnalazioniaziendali-vigilanza@bancaditalia.it; oppure
- via posta ordinaria, all'indirizzo Banca d'Italia, via Nazionale, n. 91 - 00184 Roma.

La Banca d'Italia trae da tali segnalazioni informazioni utili per le proprie funzioni di vigilanza e attiva.

Di norma, la Banca d'Italia non risponde alle segnalazioni, ma si riserva di contattare il segnalante qualora lo ritenga utile per ottenere ulteriori informazioni o chiarimenti.

La Banca d'Italia assicura la riservatezza dei dati personali del segnalante, anche al fine di tutelare quest'ultimo da possibili ritorsioni, come previsto dalla normativa in materia (art. 52-ter del TUB, art. 4- duodecies del TUF e legge n. 179 del 2017)

La Banca d'Italia, comunque, non può divulgare gli esiti degli approfondimenti condotti e le eventuali iniziative adottate a seguito di segnalazioni riguardanti intermediari vigilati, in osservanza del vincolo del segreto d'ufficio, che copre tutti i dati, le informazioni e le notizie acquisiti in ragione dell'attività di vigilanza (art. 7 del TUB).
Le segnalazioni sopra descritte (whistleblowing e aziendali) sono importanti strumenti per migliorare l'azione di vigilanza. Per la clientela che intenda invece segnalare problemi nella propria relazione commerciale con un intermediario sono previsti strumenti diversi, specificamente dedicati alla tutela degli utenti di servizi bancari e finanziari: l'esposto del cliente e il ricorso all'Arbitro Bancario Finanziario (ABF).

8. FLUSSI INFORMATIVI

Si riporta di seguito lo schema dettagliato dei Flussi Informativi minimi destinati all'OdV.

È fatto salvo qualsivoglia ulteriore flusso informativo previsto dalla normativa interna di Confidi Systema! che dovesse venire istituito a seguito dell'adozione del presente Modello.

AREA/RISCHIO	INFORMAZIONE	PERIODICITA'
RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE O L'UNIONE EUROPEA	Elenco di eventuali bandi cui si partecipa, della loro natura e delle modalità di partecipazione	Elenco inziale da aggiornare semestralmente
	Transazioni/comunicazioni/contratti con la PA o l'Unione Europea	Su richiesta dell'OdV
	Elenco delle attività ispettive effettuate dalle Autorità di Vigilanza e verbale conclusivo	Ad evento
CONTENZIOSI GIUDIZIALI O STRAGIUDIZIALI	Elenco dei contenziosi (attivi e passivi) e dei responsabili della gestione	Elenco inziale da aggiornare annualmente
TRANSAZIONI FINANZIARIE	Comunicazione di eventuali anomalie nella registrazione di fatture/ pagamenti/ incassi	Opinion della Società di revisione
	Comunicazione di eventuali irregolarità o anomalie riguardo, in particolare: al pagamento di fatture; pagamenti relativi anche alle somme da versare al fisco e agli enti previdenziali; corrispondenza tra accordi; ordini di acquisti e fatturazioni.	Opinion della Società di revisione
SELEZIONE E GESTIONE DEL PERSONALE	Report periodici sulle assunzioni, contenenti sia le modalità di selezione dei candidati utilizzate sia eventuali eccezioni/deroghe alle regole standard	Semestrale
	Elenco delle attività/programma di formazione e aggiornamento dei dipendenti	Annuale
SELEZIONE E GESTIONE DEGLI INCARICHI, DELLE CONSULENZE E PRESTAZIONI PROFESSIONALI	Elenco degli incarichi/ consulenze /prestazioni professionali di importo superiore a € 25.000,00 (esclusi organi sociali)	Annuale
REGALI, OMAGGI E SPESE DI RAPPRESENTANZA	Elenco di tutti gli omaggi/spese di rappresentanza di importo superiore al modico valore effettuati nel periodo	A richiesta
BILANCI, RELAZIONI E COMUNICAZIONI SOCIALI IN GENERE	Verbale della Società di Revisione e delle Funzioni di controllo qualora siano emerse criticità nello svolgimento delle attività di revisione	Ad evento
	Verbale di approvazione del bilancio da parte del CdA	Annuale

OPERAZIONI SOCIETARIE CHE POSSONO INCIDERE SULLA INTEGRITA' DEL CAPITALE SOCIALE	Elenco delle operazioni societarie che possono incidere sulla integrità del capitale sociale	Ad evento
	Verbali del CdA e dell'Assemblea	Ad evento
RAPPORTI CON TERZE PARTI	Comunicazione delle attività di raffronto con il mercato	Annuale
ANTIRICICLAGGIO	Elenco delle attività di controllo dei flussi finanziari aziendali in entrata	Relazione funzione antiriciclaggio
	Segnalazioni di operazioni sospette	Relazione funzione antiriciclaggio
	Informativa sui clienti censiti sull'anagrafe societaria in liste antimafia/antiterrorismo	Relazione funzione antiriciclaggio
SALUTE E DI SICUREZZA SUL LAVORO	Elenco dei soggetti incaricati al presidio della sicurezza sul lavoro: delegati, RSPP, RSL, Medico competente	Elenco iniziale e aggiornamenti ad evento
	DVR ed eventuali aggiornamenti	Annuale
	Verbale delle riunioni tra RSPP e RLS	Annuale
REATI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI	Attività di controllo e verifica della sicurezza dei sistemi informativi e sulla loro efficacia ed efficienza	Trasmissione degli esiti e delle verifiche svolte internamente
	Comunicazione degli incidenti e dei problemi relativi alla sicurezza informatica	Ad evento
	Dichiarazione di conformità sul trattamento dei dati personali	Relazione di compliance
	Copia della denuncia all'autorità giudiziaria in caso di smarrimento o furto di qualsiasi apparecchiatura informatica della Società	Ad evento

9. ALLEGATI

1. Risk Assessment 2022
2. Elenco reati