



MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. N. 231/2001

Sede legale: Strada Trossi, 38, 13871, VERRONE (BI)

Modello di Organizzazione, Gestione e Controllo

adottato ai sensi del Decreto Legislativo 8 giugno 2001, n. 231

Verrone, 26 febbraio 2016

Versione 0

Verrone, 27 gennaio 2020

Versione 1.0

Verrone, 12 gennaio 2021

Versione 2.0

Verrone, 5 marzo 2024

Versione 3.0

INDICE

INTRODUZIONE

Principi generali che hanno ispirato il lavoro di adozione del Modello	pag. 3
Finalità del Modello	pag. 3
Struttura del Modello	pag. 4

PARTE GENERALE A)

A1) Il Decreto Legislativo 8 giugno 2001, n. 231. La disciplina della responsabilità amministrativa degli Enti	pag. 5
A2) I reati ascrivibili ai soggetti sottoposti all'altrui vigilanza o agli apicali; gli illeciti amministrativi ascrivibili alla società	pag. 6
A3) Le sanzioni previste dal Decreto: articoli 9, 10, 11, 12, 13 e 14	pag. 8
A4) I requisiti per escludere la responsabilità amministrativa dell'ente	pag. 10
A5) Le caratteristiche normative del Modello	pag. 12

PARTE SPECIALE B)

Il Modello di Organizzazione, Gestione e Controllo di ALLSYSTEM

B1) L'attività e la struttura organizzativa di ALLSYSTEM	pag. 14
B2) I presupposti del Modello	pag. 15
B3) L'aggiornamento del Modello	pag. 18
B4) La mappa delle attività a rischio del Modello adottato in data 26.02.2016	pag. 19
B5) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2019	pag. 21
B6) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2020	pag. 22
B7) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2023	pag. 24
B8) Il Codice Etico	pag. 26
B9) I protocolli di decisione	pag. 26
B10) L'Organismo di Vigilanza	pag. 27
B10 – I) Caratteristiche dell'Organismo di Vigilanza	pag. 27
B10 – II) Composizione, durata e compensi dell'Organismo di Vigilanza	pag. 28
B10 – III) Requisiti di eleggibilità, cause di decadenza e sospensione. Requisiti di onorabilità	pag. 28
B10 – IV) Compiti dell'Organismo di Vigilanza	pag. 31
B10 – V) Modalità e periodicità di riporto agli Organi Societari	pag. 32
B10 – VI) Flussi informativi verso l'Organismo di Vigilanza	pag. 33
B11) Designazione del Gestore del canale di segnalazione interno	pag. 38
B12) Il sistema disciplinare	pag. 39
Principi generali	pag. 39
B12 – I) Personale dipendente (art. 101 e seguenti CCNL)	pag. 41
B12 – II) Dirigenti	pag. 45
B12 – III) Componenti del Consiglio di Amministrazione	pag. 45
B12 – IV) Componenti del Collegio Sindacale	pag. 46
B12 – V) Soggetti esterni	pag. 46
B13) La diffusione del Modello	pag. 46
B13 – I) Il piano di comunicazione	pag. 46
B13 – II) Il piano di formazione	pag. 47
B14) L'aggiornamento del Modello	pag. 47

INTRODUZIONE

Principi generali che hanno ispirato il lavoro di adozione del Modello

ALLSYSTEM S.p.a. (di seguito anche la “Società”), sensibile all’esigenza di assicurare condizioni di correttezza e di trasparenza nella conduzione degli affari e delle attività aziendali, a tutela della posizione e dell’immagine propria nonché delle aspettative dei propri soci e dei propri dipendenti, ha ritenuto opportuno analizzare, compendiare e rafforzare tutti gli strumenti di controllo già adottati e, conseguentemente, apportare gli adeguamenti richiesti procedendo all’attuazione del Modello di organizzazione, gestione e controllo, previsto dal D.Lgs. n. 231/2001 (di seguito anche il “Modello”).

Il presente documento, corredato di tutti i suoi Allegati, illustra il Modello adottato dal Consiglio di Amministrazione di ALLSYSTEM S.p.a. con delibera del 26/02/2016 ai sensi del Decreto Legislativo 8 giugno 2001, n. 231 (di seguito il “Decreto” o il “D.Lgs. 231/2001”).

Alla luce delle novelle legislative che hanno in parte innovato e in parte modificato le disposizioni del Decreto, intervenute a più riprese a seguito della prima adozione del Modello, si è reso necessario procedere a una serie di successivi aggiornamenti dello stesso a mezzo di integrazioni che coinvolgono sia la parte generale che la parte speciale, oltre al Codice Etico e ai protocolli di decisione.

Così come riportato nel presente documento, il Modello rappresenta il sistema di regole organizzative, operative e di controllo che disciplinano l’attività e i comportamenti della Società per prevenire i reati e gli illeciti amministrativi rilevanti ai sensi del Decreto, integrando e completando il sistema di attribuzione di funzioni e di poteri e il sistema dei controlli interni attualmente in vigore.

Finalità del Modello

Con l’adozione ed il conseguente aggiornamento del presente Modello, ALLSYSTEM si propone di perseguire le seguenti finalità:

- ribadire che ogni condotta illecita è fortemente condannata e mai giustificata dalla Società, anche se ispirata ad un supposto interesse sociale ed anche se la Società sia apparentemente in condizione di trarne vantaggio o averne interesse;
- determinare, in tutti coloro che operano in nome e per conto di ALLSYSTEM e, in particolare, nelle aree individuate “a rischio” di realizzazione dei reati, la consapevolezza dell’obbligo di dover rispettare le regole aziendali e di poter incorrere, in caso di violazione delle medesime, nella commissione di illeciti passibili di sanzioni penali comminabili nei loro stessi confronti e di sanzioni penali-amministrative irrogabili all’azienda;

- consentire alla Società, grazie ad un'azione di stretto controllo e monitoraggio sulle aree di attività sensibili, di intervenire tempestivamente per prevenire o contrastare la commissione dei reati stessi.

Struttura del Modello

Il presente documento si compone di due sezioni, debitamente aggiornate alla luce delle innovazioni legislative a cui è stato sottoposto il Decreto a seguito della sua adozione:

- **Parte Generale A)**: descrive i contenuti del Decreto Legislativo 8 giugno 2001, n. 231, illustra i reati e gli illeciti amministrativi che determinano la responsabilità amministrativa della Società, le possibili sanzioni e le condizioni per l'esenzione della responsabilità;
- **Parte Speciale B)**: descrive il modello di controllo interno e di organizzazione e gestione specifico della Società (modalità di costruzione, diffusione e aggiornamento), identifica la struttura, i ruoli e le responsabilità dell'Organismo di Vigilanza e illustra il sistema disciplinare interno finalizzato a sanzionare il mancato rispetto delle regole previste dal Modello stesso.

Costituiscono parte integrante del Modello i seguenti Allegati, sottoposti ad aggiornamento sulla base delle novità legislative introdotte in materia di responsabilità amministrativa degli enti:

- l'elenco dei reati e degli illeciti amministrativi rilevanti ai sensi del D.Lgs. 231/2001 **(Allegato 1)**;
- il Codice Etico della Società **(Allegato 2)**;
- procedura "Whistleblowing" **(Allegato 3)**;
- documento di Risk Assessment **(Allegato 4)**;
- i protocolli di decisione elaborati, ad oggi, nelle aree ritenute più sensibili nella prospettiva della responsabilità amministrativa della Società **(Allegato 5)**;

I Destinatari del Modello adottato da ALLSYSTEM.

Le regole contenute nel Modello si applicano agli amministratori, ai soci e a tutti gli esponenti aziendali, ai dipendenti, ai consulenti, a coloro che collaborano stabilmente con la Società e a tutto il personale della Società ed in particolare a coloro che svolgono, anche di fatto, le attività a rischio ai sensi del Decreto.

I collaboratori esterni, i fornitori, i consulenti, e gli eventuali partner commerciali di ALLSYSTEM sono tenuti al rispetto delle prescrizioni dettate dal Decreto e dei principi etici adottati ed esplicitati nel Codice Etico della Società anche attraverso la sottoscrizione di apposite clausole contrattuali.

Specularmente, ALLSYSTEM selezionerà i propri fornitori, soci, partner commerciali verificando che in capo ai medesimi non esistano precedenti specifici per responsabilità

amministrativa ai sensi del Decreto 231/2001, chiedendo loro di autocertificare l'incensuratezza o meno ai sensi del Decreto.

PARTE GENERALE A)

A1) Il Decreto Legislativo 8 giugno 2001, n. 231. La disciplina della responsabilità amministrativa degli Enti

Il Decreto Legislativo 8 giugno 2001 n. 231 *“Disciplina della responsabilità amministrativa delle persone giuridiche delle società e delle associazioni anche prive di personalità giuridica”*, in attuazione della delega conferita al Governo con l'art. 11 della Legge 29 settembre 2000, n. 300¹, disciplina la *“responsabilità degli enti per gli illeciti amministrativi dipendenti da reato”*, che si applica agli enti dotati di personalità giuridica e alle società e associazioni anche prive di personalità giuridica.

Il Decreto, in vigore dal 4 luglio 2001, ha introdotto la responsabilità amministrativa degli Enti in aggiunta alla responsabilità penale della persona fisica che ha commesso il reato nell'interesse o a vantaggio dell'ente medesimo (art. 5, 1° comma del Decreto).

Secondo la disciplina introdotta dal Decreto, infatti, gli Enti possono essere ritenuti responsabili per alcuni reati, tassativamente indicati dalle norme, nella forma consumata o tentata, nell'interesse o a vantaggio degli stessi Enti e a prescindere dal conseguimento degli stessi, sia da coloro che, in posizione apicale, rivestano, anche di fatto, funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua Unità Organizzativa dotata di autonomia finanziaria e funzionale, sia da coloro che sono sottoposti alla direzione o vigilanza dei primi (questo il contenuto dettato dall'art. 5, comma 1, lettere a) e b) del D. Lgs. n. 231/2001)².

Come meglio precisato in seguito, l'esclusione della predetta responsabilità può essere riconosciuta all'Ente che abbia adottato ed efficacemente attuato un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire la realizzazione di reati, in virtù di quanto separatamente previsto dal Decreto stesso per gli apicali sub art. 6, 1° comma e, per i

¹ La legge 29 settembre 2000, n. 300, nel delegare al governo la definizione di un sistema di responsabilità sanzionatoria amministrativa degli enti e delle società, ha ottemperato agli obblighi previsti da alcuni protocolli e convenzioni internazionali ratificate dall'Italia, relative alla responsabilità degli enti collettivi per talune fattispecie di reato, tra le quali la Convenzione sulla tutela degli interessi finanziari delle comunità europee (Bruxelles, 26 luglio 1995) e relativo primo Protocollo (Dublino, 27 settembre 1996), la Convenzione relativa alla lotta contro la corruzione nella quale sono coinvolti funzionari delle comunità europee o degli Stati membri dell'Unione Europea (Bruxelles, 26 maggio 1997), la Convenzione OCSE sulla lotta alla corruzione di pubblici ufficiali stranieri nelle operazioni economiche internazionali (Parigi, 17 dicembre 1997).

² Art. 5, comma 1, del D.Lgs. n. 231/2001: *“Responsabilità della società – La società è responsabile per i reati commessi nel suo interesse o a suo vantaggio: a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione della società o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a)”*.

dipendenti o le persone sottoposte all'altrui direzione e vigilanza sub art. 7, 1°, 2° e 3° comma.

A2) I reati ascrivibili ai soggetti sottoposti all'altrui vigilanza o agli apicali; gli illeciti amministrativi ascrivibili alla società

In base al Decreto, l'Ente può essere ritenuto responsabile soltanto per i fatti costituenti reato espressamente richiamati da specifiche disposizioni normative entrate in vigore prima della commissione dei fatti stessi, mutuando il principio di legalità vigente in materia strettamente penalistica e prescritto dalla stessa Carta Costituzionale nell'art. 25 Cost.

Nel corso degli anni si è assistito ad un progressivo ampliamento del novero dei reati e dei conseguenti illeciti presupposto con riferimento ai quali si applica la normativa in esame.

Le fattispecie richiamate dal D.Lgs. n. 231/2001 possono essere comprese, per comodità espositiva, nei seguenti macrogruppi di reati³, di cui si evocano alcuni esempi di comune conoscenza, rimandando all'allegato sub 1) l'elenco analitico di tutte le fattispecie:

- reati contro la Pubblica Amministrazione, come la corruzione, la concussione, l'induzione indebita a dare o promettere utilità, il traffico di influenze illecite (fattispecie di reato, quest'ultima, profondamente innovata dalla L. 9 gennaio 2019 n. 3, che ne ha peraltro determinato l'inserimento nel novero dei reati presupposto all'art. 25 del Decreto), la truffa aggravata ai danni di enti pubblici, la malversazione di denaro pubblico, la frode nelle pubbliche forniture (fattispecie di reato inserita nel novero degli illeciti presupposto all'art. 25 del Decreto ad opera del D.Lgs. 14 luglio 2020 n. 75), la turbata libertà degli incanti e la turbata libertà del procedimento di scelta del contraente (fattispecie di reato inserite nel novero degli illeciti presupposto all'art. 24 del Decreto ad opera del D.L. 10.08.2023 n. 105 (convertito con modificazioni dalla L. 9.10.2023 n. 137));
- reati tributari ricompresi nel catalogo degli illeciti presupposto all'art. 25 *quinquiesdecies* del Decreto ad opera del D.L. 26 ottobre 2019 n. 124 (convertito con modificazioni nella L. 19 dicembre 2019 n. 157) e del D.Lgs. 14 luglio 2020 n. 75;
- reati di contrabbando inseriti nel novero degli illeciti presupposto all'art. 25 *sexiesdecies* del Decreto ad opera del D.Lgs. 14 luglio 2020 n. 75;
- delitti informatici, quali l'accesso abusivo a sistemi informatici o telematici, l'alterazione della altrui firma digitale;
- delitti in materia di strumenti di pagamento diversi dai contanti e trasferimento fraudolento di valori inseriti nel novero degli illeciti presupposto all'art. 25 *octies1* del Decreto ad opera del D.Lgs. 8 novembre 2021 n. 184 nonché del D.L. 10 agosto 2023 n. 105 (convertito con modificazioni dalla L. 9.10.2023 n. 137);

³ Per il dettaglio dei reati ed i reati presupposto raggruppati per ogni articolo dall'art. 24 all'art. 25 *duodevices* si rimanda all'Allegato 1 "I reati e gli illeciti amministrativi per i quali trova applicazione il D.Lgs. n. 231/2001".

- reati di criminalità organizzata, come l'associazione per delinquere di stampo mafioso o l'associazione per delinquere finalizzata alla commissione di reati contro la persona;
- falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento;
- frode informatica con sostituzione dell'identità digitale, in vigore dall'agosto 2013;
- delitti contro l'industria e il commercio, come la frode in commercio, in vigore dal 2009;
- reati societari, come le false comunicazioni sociali, l'infedeltà patrimoniale, l'illecita ripartizione degli utili, la cosiddetta corruzione tra privati (art. 2635 c.c. modificato dal D.Lgs. 15 marzo 2017, n. 38) nonché di istigazione alla corruzione tra privati (introdotto all'art. 2635 *bis* c.c. dal D.Lgs. 15 marzo 2017, n. 38 e inserito nel novero dei reati presupposto alla lettera *s bis*) dell'art. 25 *ter* del Decreto, unitamente al già compendiato art. 2635 c.c.);
- reati con finalità di terrorismo o di eversione dell'ordine democratico;
- pratiche di mutilazione degli organi genitali femminili;
- delitti contro la personalità individuale come la riduzione in schiavitù, prostituzione minorile, l'intermediazione illecita o sfruttamento del lavoro (reato introdotto all'art. 603 *bis* c.p. dalla L. 29 ottobre 2016, n. 199 e parimenti inserito nel novero dei reati presupposto all'art. 25 *quinquies*, comma 1, lett a) del Decreto), pornografia minorile, detenzione di materiale pedopornografico, adescamento di minorenni, reati introdotti nel 2003 e nel 2014;
- abusi di mercato, e specificatamente *l'insider trading* e la manipolazione del mercato;
- reati di lesioni e omicidio colposi commessi con violazione della normativa sulla sicurezza sul lavoro, introdotti nel 2007;
- reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, introdotti con la L. 21 novembre 2007 n. 231, e di autoriciclaggio, introdotto con la L. 15 dicembre 2014 n. 186;
- delitti contro il patrimonio culturale e delitti di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici inseriti nel novero degli illeciti presupposto rispettivamente agli artt. 25 *septiesdecies* e 25 *duodevicies* del Decreto ad opera della Legge 9 marzo 2022 n. 22;
- indebito utilizzo, falsificazione, alterazione e ricettazione di carte di credito o di pagamento;
- reati di violazione del diritto d'autore;
- reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, ovvero il delitto di cui all'art. 377 *bis* c.p.;
- reati ambientali, introdotti nel 2011 e recentemente novellati e ampliati nel 2015 anche ai fini della responsabilità amministrativa;

- reati transnazionali;
- reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare come l'occupazione di lavoratori stranieri privi del permesso di soggiorno o con permesso di soggiorno scaduto o non rinnovato, revocato o annullato; procurato ingresso illecito dello straniero nel territorio dello Stato e favoreggiamento della permanenza clandestina dello straniero nel territorio dello stato (fattispecie di reato, le ultime due, inserite ad opera della L. 17 ottobre 2017, n. 161 nel novero dei reati presupposto all'art. 25 *duodecies*, rispettivamente ai commi 1 *bis* e 1 *ter* del Decreto);
- reati commessi con finalità di razzismo e xenofobia (fattispecie di reato inserita nel catalogo degli illeciti presupposto ad opera della L. 20 novembre 2017 n. 167 all'art. 25 *terdecies* del Decreto).

Tali reati possono comportare la responsabilità amministrativa dell'Ente avente sede principale nel territorio italiano anche se commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto e nei limiti e alle condizioni previsti dal codice penale sub artt. 7, 8, 9 e 10 per i reati commessi all'estero dallo straniero ai danni dello Stato italiano o dal cittadino italiano⁴.

A3) Le sanzioni previste dal Decreto: articoli 9, 10, 11, 12, 13 e 14

Il Decreto prevede a carico degli Enti, in conseguenza della commissione o tentata commissione (l'art. 26 del decreto riproduce la disciplina del delitto tentato di cui all'art. 56 c.p.) dei reati sopra menzionati, una serie predeterminata e articolata di sanzioni classificabili in quattro tipologie:

- sanzioni pecuniarie (artt. 9, 10, 11 e 12 del Decreto): si applicano ogniqualvolta venga accertata la responsabilità della persona giuridica e sono determinate dal giudice attraverso un sistema basato su «quote» dal valore predeterminato. Nell'ambito di un minimo e di un massimo di quote indicate dal legislatore per ciascun reato nonché del valore da attribuire ad esse, il Giudice stabilisce l'ammontare delle sanzioni pecuniarie tenendo conto 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, come prevede l'art. 11 del Decreto analogamente a quanto è chiamato a fare il Giudice nell'irrogare le pene principali valutando il fatto alla stregua dei parametri di cui all'art. 133 c.p.;

⁴ L'art. 4 del D.Lgs. 231/2001, sotto la rubrica "reati commessi all'estero", prevede: "1. nei casi e alle condizioni previsti dagli articoli 7, 8, 9 e 10 del codice penale, gli enti aventi nel territorio dello Stato la sede principale rispondono anche in relazione ai reati commessi all'estero, purché nei loro confronti non proceda lo Stato del luogo in cui è stato commesso il fatto. 2. Nei casi in cui la legge prevede che il colpevole sia punito a richiesta del Ministro della Giustizia, si procede contro l'ente solo se la richiesta è formulata nei confronti di quest'ultimo".

- sanzioni interdittive (artt. 13, 14, 15 e 16 del Decreto): possono trovare applicazione per alcune tipologie di reato e per le ipotesi di maggior gravità, allorché l'ente abbia tratto dal reato un profitto di considerevole entità. Si traducono nell'interdizione dall'esercizio dell'attività aziendale; nella sospensione e nella revoca delle autorizzazioni, delle licenze o delle concessioni funzionali alla commissione dell'illecito; nel divieto di contrattare con la pubblica amministrazione (salvo che per ottenere le prestazioni di un pubblico servizio); nell'esclusione da agevolazioni, finanziamenti, contributi o sussidi e nell'eventuale revoca di quelli concessi; nel divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive non si applicano, secondo quanto prevede l'art. 17 del Decreto, (o sono revocate, se già applicate in via cautelare⁵) qualora l'Ente, prima della dichiarazione di apertura del dibattimento di primo grado, abbia, congiuntamente:

- risarcito il danno o lo abbia riparato;
- eliminato le conseguenze dannose o pericolose del reato (o, almeno, si sia adoperato in tal senso);
- messo a disposizione dell'Autorità Giudiziaria, per la confisca, il profitto del reato;
- eliminato le carenze organizzative che hanno determinato il reato, adottando Modelli organizzativi idonei a prevenire la commissione di nuovi reati.

Le sanzioni interdittive si applicano quando ricorre almeno una delle seguenti condizioni, ex art. 13 del Decreto:

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

Le sanzioni interdittive, secondo il regime ordinario stabilito dall'art. 13, comma 2 del Decreto, hanno durata non inferiore a tre mesi e non superiore a tre anni.

⁵ Due le deroghe alla applicabilità incondizionata in via cautelare delle misure interdittive: il D.Lgs. 9 luglio 2004 n. 197 ha inserito nel T.U.B. la nuova Sezione V-bis (Responsabilità per illecito amministrativo dipendente da reato), che contiene un solo articolo (97-bis) che vieta l'applicazione, in via cautelare, delle sanzioni dell'interdizione dall'esercizio dell'attività, della sospensione/revoca delle autorizzazioni e del commissariamento giudiziale ex art 15 D.Lgs. 231/2001. Stessa soluzione viene operata dal D.Lgs. 197/2004 per il T.U.F., che viene novellato con l'aggiunta di un nuovo art 60-bis (Responsabilità delle SIM, delle SGR e delle SICAV per illecito amministrativo dipendente da reato).

Si rileva, per inciso, che la L. 9 gennaio 2019 n. 3 (*Misure per il contrasto dei reati contro la pubblica amministrazione, nonché in materia di prescrizione del reato e in materia di trasparenza dei partiti e movimenti politici*) ha inasprito la durata delle sanzioni interdittive, come *ab origine* disciplinata dal precitato articolo, dei reati presupposto previsti dall'art. 25, commi 2 e 3 del Decreto ossia dei reati contro la Pubblica Amministrazione reputati di maggior allarme sociale.

In particolare, il comma 5 dell'art. 25 del Decreto, come modificato dalla L. n. 3/2019, sancisce che, nel caso di condanna per le predette ipotesi di reato, le sanzioni interdittive abbiano una durata di:

1. non inferiore a quattro anni e non superiore a sette anni, se il reato è stato commesso da uno dei soggetti di cui all'art. 5, comma 1, lett. a) del Decreto;
2. non inferiore a due anni e non superiore a quattro anni, se il reato è stato commesso da uno dei soggetti di cui all'art. 5, comma 1, lett. b) del Decreto;

Ai sensi del comma 5 *bis* dell'art. 25 del Decreto, introdotto dalla L. n. 3/2019, l'inasprimento delle sanzioni interdittive in relazione ai reati presupposto succitati non avrà luogo, riespandendosi di conseguenza il regime ordinario previsto dall'art. 13, comma 2 del Decreto, qualora 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 trasferite 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.

- Confisca del prezzo o del profitto del reato (art. 19 del Decreto): consiste nell'acquisizione del prezzo o del profitto del reato da parte dello Stato o nell'acquisizione di somme di denaro, beni o altre utilità di valore equivalente al prezzo o al profitto del reato: non investe, tuttavia, quella parte del prezzo o del profitto del reato che può restituirsi al danneggiato e sono fatti salvi i diritti acquisiti dai terzi in buona fede. La confisca è sempre disposta con la sentenza di condanna.
- Pubblicazione della sentenza di condanna in uno o più giornali indicati dal Giudice nella sentenza, nonché mediante affissione nel comune ove l'Ente ha la sede principale (art. 18 del Decreto). Può essere inflitta come pena accessoria nel caso in cui vengano irrogate sanzioni interdittive.

A4) I requisiti per escludere la responsabilità amministrativa dell'ente

Il Decreto prevede, all'articolo 6, che gli Enti non rispondono del reato commesso nel loro interesse o vantaggio da uno dei soggetti apicali qualora siano in grado di provare:

- (i) di aver adottato ed efficacemente attuato, prima della commissione del reato, un modello di organizzazione e gestione idoneo a prevenire la commissione di reati della specie di quello verificatosi;
- (ii) di aver affidato ad un proprio organismo, dotato di autonomi poteri di iniziativa e controllo, il compito di vigilare sul funzionamento e l'osservanza del modello e di curarne l'aggiornamento (cosiddetto Organismo di Vigilanza su cui *infra*);
- (iii) che la commissione del reato da parte dei soggetti apicali si è verificata solo a seguito dell'elusione fraudolenta del predisposto modello di organizzazione e gestione;
- (iv) che la commissione del reato non è stata conseguente ad una omessa o insufficiente vigilanza da parte dell'Organismo di Vigilanza.

Nel caso in cui, invece, il reato venga commesso da soggetti sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra indicati, l'Ente è responsabile se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione o vigilanza. In tale ipotesi, ai sensi dell'articolo 7 del Decreto, l'adozione ed efficace attuazione di un modello di organizzazione e gestione volto alla prevenzione dei reati della specie di quello verificatosi ha, di per sé, efficacia esimente da responsabilità per l'Ente.

Ai sensi degli articoli 12 e 17 del Decreto l'adozione di un modello di organizzazione e di gestione rileva, oltre che come possibile esimente per l'Ente dalla responsabilità amministrativa se idoneamente adottato prima della commissione del fatto, anche, in via subordinata, ai fini della riduzione della sanzione pecuniaria e della inapplicabilità delle sanzioni interdittive, purché esso sia adottato in un momento anteriore alla dichiarazione di apertura del dibattimento di primo grado e risulti idoneo a prevenire la commissione dei reati della specie di quelli verificatisi. Ulteriore condizione, la messa a disposizione del profitto conseguito ai fini della confisca.

Gli elementi qualificanti del modello di organizzazione e gestione di un Ente, ai sensi del secondo comma dell'articolo 6 del Decreto, sono:

- (i) mappa delle attività nel cui ambito possono essere commessi i reati previsti dal Decreto (gap analysis o mappatura del rischio reato);
- (ii) protocolli volti a programmare la formazione e l'attuazione delle decisioni dell'ente in relazione ai reati da prevenire (protocolli di decisione);
- (iii) procedure finalizzate a disciplinare le modalità di gestione delle risorse finanziarie, idonee ad impedire che si verifichino situazioni atte a favorire la commissione di reati, quali tipicamente la creazione di fondi occulti con fatture soggettivamente o oggettivamente false o la gestione non tracciata di denaro contante;
- (iv) obblighi di informazione da parte dei responsabili delle funzioni aziendali nei confronti dell'organismo deputato a vigilare sul funzionamento del Modello (cosiddetti flussi informativi da e verso l'Organismo di Vigilanza);
- (v) sistema disciplinare idoneo a sanzionare il mancato rispetto delle disposizioni del Modello, al fine di garantirne l'efficace attuazione.

Il Modello di organizzazione, gestione e controllo consiste, pertanto, in un insieme di regole comportamentali e di principi di controllo volti alla prevenzione della realizzazione dei comportamenti illeciti rilevanti ai sensi del Decreto e a garantire lo svolgimento delle attività aziendali nel rispetto della legge ed in una serie di meccanismi di segnalazione e comunicazione delle intervenute violazioni alle suddette regole e principi.

A5) Le caratteristiche normative del Modello

In linea di massima il Decreto non disciplina analiticamente i contenuti precettivi e non del Modello di organizzazione, gestione e controllo: esso si limita prevalentemente a dettare alcuni principi di ordine generale parametrati in funzione dei differenti soggetti che potrebbero realizzare un illecito. In particolare, per la prevenzione degli illeciti presupposto, il Modello deve rispondere alle seguenti esigenze dettate dall'art. 6 comma 2 del Decreto:

1. individuare le attività nel cui ambito possono essere commessi illeciti;
2. prevedere specifici protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'ente, in relazione agli illeciti da prevenire;
3. individuare modalità di gestione delle risorse finanziarie idonee ad impedire la commissione di illeciti;
4. prevedere obblighi di informazione nei confronti dell'organismo deputato a vigilare sul funzionamento e l'osservanza dei modelli;
5. introdurre un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Il Modello ai sensi dell'art. 7 comma 3 del Decreto deve altresì prevedere *“in relazione alla natura e alla dimensione dell'organizzazione, nonché al tipo di attività svolta, misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a scoprire ed eliminare tempestivamente situazioni di rischio”*.

Con riferimento all'efficace attuazione del Modello, l'articolo 7 comma 4 del Decreto richiede:

1. una verifica periodica e l'eventuale modifica dello stesso quando sono scoperte significative violazioni delle prescrizioni ovvero quando intervengono mutamenti nell'organizzazione o nell'attività;
2. un sistema disciplinare idoneo a sanzionare il mancato rispetto delle misure indicate nel modello.

Maggiore analiticità – in punto contenuti e caratteristiche del Modello – caratterizza la disciplina contenuta nel Decreto concernente le segnalazioni (da parte dei Destinatari del

Modello e/o Procedura *Whistleblowing*) di possibili condotte rilevanti ai fini del medesimo (c.d. *Whistleblowing*).

A questo proposito il comma 2 *bis* dell'art. 6 del Decreto – vigente sino al 14 luglio 2023 – disponeva che i Modelli dovessero prevedere:

- a) uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b) (ovvero apicali e dipendenti), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del Decreto 231 e fondate su elementi di fatto precisi e concordanti, o di violazioni del Modello di Organizzazione e Gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;
- b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;
- c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
- d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

A far data dal 15 luglio 2023 il sopra richiamato comma 2 *bis* dell'art. 6 del Decreto assume per società come ALLSYSTEM (ovvero con un numero di lavoratori subordinati superiore alle 249 unità) un diverso contenuto recependo, in punto comunicazioni/segnalazioni di fatti rilevanti (anche) ai fini del Decreto, la Direttiva UE 2019/1937. Infatti il comma 2 *bis* dell'art. 6 del Decreto nella versione recentemente novellata dal D. Lgs. 10 marzo 2023 n. 24 così recita: *"I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)"*.

Ciò premesso, ai fini delle segnalazioni c.d. "Whistleblowing" ALLSYSTEM ha inteso conformarsi alle previsioni della Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019 e relativa normativa attuativa nazionale (D. Lgs. n. 24/2023). Si rammenta che la normativa domestica riguardante il *Whistleblowing* emanata in attuazione della citata disciplina comunitaria appresta una specifica protezione delle persone che segnalano violazioni di disposizioni normative nazionali o comunitarie che ledono l'interesse pubblico o l'integrità dell'ente privato (nel caso di specie ALLSYSTEM) di cui siano venute a conoscenza in un contesto lavorativo. Tale normativa fornisce una disciplina organica delle segnalazioni riguardanti non solo violazioni rilevanti ai fini della disciplina dettata dal Decreto n. 231/2001, bensì anche condotte (attive od omissive) integranti illeciti amministrativi, contabili, civili o penali (e, quanto a questi ultimi, anche reati non

presupposto cioè non implicanti responsabilità amministrativa per l'Ente). In sostanza con il D. Lgs. n. 24/2023 è stato disciplinato nella sua interezza il fenomeno della segnalazione (riservata) sia di quelle violazioni rilevanti ai fini del D. Lgs. n. 231/2001 che di quelle potenzialmente 'nocive' per gli enti (pubblici o privati).

In tale prospettiva è dunque interesse della ALLSYSTEM adottare una soluzione organizzativa che si riveli perfettamente in linea rispetto alla nuova normativa sul c.d. *Whistleblowing* e idonea a fornire attuazione sia alle esigenze di segnalazione riservata ai fini del D. Lgs. n. 231/2001 sia alle ulteriori esigenze mutate nel D. Lgs. n. 24/2023.

A fronte di ciò, ALLSYSTEM, in occasione dell'opera di aggiornamento del presente Modello avviata nel 2023, ha adottato un sistema di segnalazione delle violazioni da subito conforme alla normativa comunitaria (per come recepita dal legislatore italiano) che consente pertanto di recepire sia segnalazioni di violazioni rilevanti ai soli fini del D. Lgs. n. 231/2001 sia segnalazioni di violazioni rilevanti agli altri fini di cui al D. Lgs. n. 24/2023.

Il citato sistema di segnalazione adottato da ALLSYSTEM è disciplinato in apposta Procedura *Whistleblowing* facente parte del Modello Organizzativo e di Gestione della Società (allegato n. 3) e pubblicata sul sito internet della Società nella sezione Sistemi Aziendali.

PARTE SPECIALE B)

Il Modello di Organizzazione, Gestione e Controllo di ALLSYSTEM

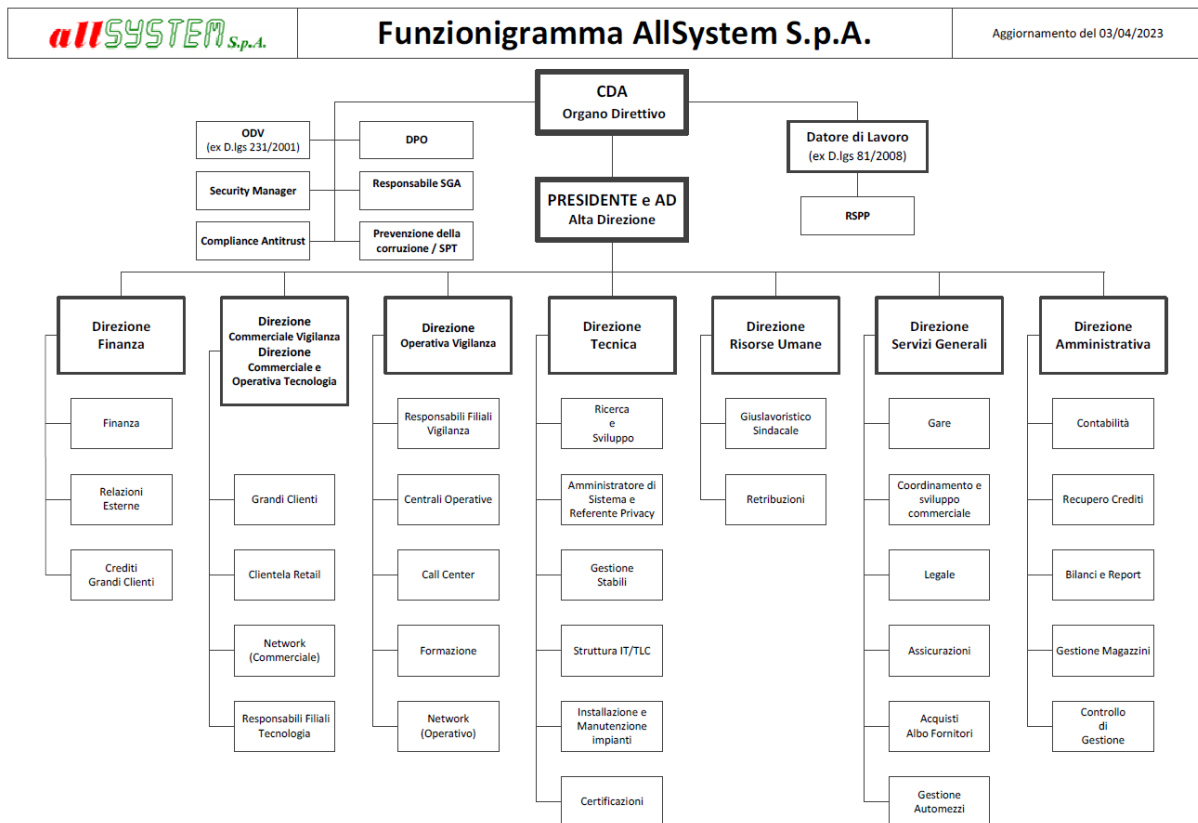
B1) L'attività e la struttura organizzativa di ALLSYSTEM.

ALLSYSTEM S.p.a. è una realtà imprenditoriale che opera sul territorio nazionale nel settore della vigilanza privata e della sicurezza; fino al luglio 2020 svolgeva vari tipi di servizi, come i servizi di scorta a trasporti effettuati da terzi, servizi di scorta e trasporto valori; ad oggi tale attività è cessata a seguito di vendita del ramo aziendale e l'attività di impresa prosegue con servizi di portierato presso enti pubblici e privati, servizi di guardiania notturna e diurna di beni immobili e obiettivi strategici, servizi di vigilanza, servizi ispettivi e di intervento su segnalazione d'allarme, servizi di ricezione e gestione allarmi. Parte del suo *business* consiste, a fronte dell'incorporazione dell'intero ramo aziendale di AllSystem 1 S.r.l., nella progettazione, l'installazione, la vendita e il noleggio, la manutenzione di sistemi di sicurezza e di allarme, impianti tecnici elettrici ed elettronici in sedi civili e industriali; non svolge più dal luglio 2020, per le ragioni sopra accennate, servizi di custodia, deposito e contazione di monete, banconote, valori mobiliari e titoli di credito per conto di primari clienti della grande distribuzione e del mondo bancario.

L'ampia e diversificata offerta di servizi fanno tuttora di ALLSYSTEM un soggetto imprenditoriale da tempo impegnato nella sorveglianza di enti pubblici strategici (come le Regioni, le Province, i Comuni, i palazzi di giustizia), molto ramificato sul territorio nazionale

[potendo annoverare le filiali di Alessandria, Aosta, Asti, Cuneo, San Pietro Mosezzo (NO), Bergamo, Genova, Vercelli, Milano, Busto Arsizio (VA), Verrone (BI), Torino] spesso coinvolto da partner commerciali in associazioni di imprese o network di vigilanza.

ALLSYSTEM presenta una struttura organizzativa chiaramente definita come è evidenziato nel funzionigramma posto di seguito.



B2) I presupposti del Modello.

La decisione di adottare un Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, nonché di operare le opportune revisioni dello stesso, aggiornandolo alla luce delle novità legislative significative e rivalutandolo al fine di apportarvi i correttivi sulla base della prassi consolidatasi nei circa otto anni di vigenza dello stesso Modello, oltre a rappresentare un motivo di esenzione dalla responsabilità amministrativa della Società con riferimento alla commissione di alcune tipologie di reato presupposto, è un atto di responsabilità sociale che rientra nel quadro di un impegno più generale che la Società ha assunto sia nei confronti dei propri soci, clienti, dipendenti, collaboratori, fornitori, concorrenti ed altri partner d'affari, sia nei confronti degli enti pubblici, a partecipazione pubblica e con gli altri soggetti committenti della Società.

Conseguentemente, nell'originaria predisposizione e nella successiva fase di aggiornamento e di rivalutazione del presente Modello si è tenuto innanzitutto conto della normativa vigente, delle prassi, delle procedure e dei sistemi di controllo esistenti e già operanti in ALLSYSTEM, nonché dei protocolli decisionali elaborati e adottati nel quadriennio di vigenza del presente Modello.

È evidente che il sistema di governo e controllo societario già esistente, costituisce, infatti, un prezioso strumento a presidio della prevenzione di comportamenti illeciti in genere, inclusi quelli previsti dalla normativa specifica che dispone la responsabilità amministrativa degli enti.

Quali specifici strumenti già esistenti e diretti a programmare la formazione e l'attuazione delle decisioni aziendali e ad effettuare i controlli sulle attività aziendali, ALLSYSTEM ha individuato i seguenti:

- sistema di governo societario;
- sistema dei poteri e delle deleghe in capo ai componenti del consiglio di amministrazione e ai responsabili delle singole direzioni, ai Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010 ed ai responsabili di filiale;
- sistema di controllo interno.

Il sistema di governo societario.

Le regole che disciplinano l'attività di ALLSYSTEM sono state adottate in recepimento della normativa societaria e, in particolare, la *governance* societaria è affidata a:

- Presidente del Consiglio di Amministrazione che riveste anche l'incarico di Amministratore Delegato;
- il Datore di lavoro ai sensi del Decreto Legislativo n. 81/2008;
- Amministratori e Consiglieri Delegati.

Il sistema dei poteri

Il sistema dei poteri di ALLSYSTEM, documentato attraverso il funzionigramma di cui al paragrafo precedente nonché attraverso le procure e le deleghe formalmente attribuite ai Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010, ai responsabili di filiale e ai responsabili delle direzioni (finanza, commerciale, operativa, tecnica, risorse umane, servizi generali e amministrativa), è improntato ai criteri di formalizzazione e chiarezza, attribuzione di ruoli e responsabilità, separazione/segregazione delle attività operative e di controllo, definizione delle linee gerarchiche e delle attività operative.

Solo i soggetti muniti di formali e specifici poteri possono assumere impegni verso i terzi in nome e per conto della Società.

In particolare, il Consiglio di Amministrazione ha attribuito cariche e poteri al Presidente e agli Amministratori Delegati attribuendo loro distinte deleghe anche in materia di tutela della sicurezza sul lavoro e considerando anche la modalità di esercizio della firma (disgiunta salvo atti di straordinaria amministrazione tassativamente indicati).

Sono inoltre attribuite, tramite atti notarili, le necessarie procure generali in capo ai Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010, ai responsabili di filiale e ai responsabili delle diverse direzioni.

L'attuale organigramma della Società, nell'arco degli otto anni di adozione del Modello, non ha subito significative modifiche tali da dover riconsiderare, sotto tale aspetto, i protocolli decisionali già adottati nelle aree di competenza dell'attività societaria. Le funzioni e le cariche principali, a cui continuano ad essere attribuiti poteri decisionali, risultano invariate, diversamente da quanto occorre per alcune funzioni alle prime sottoposte.

Il sistema di controllo interno

Il sistema di controllo interno di ALLSYSTEM è costituito, *in primis*, dalle procedure mutate nei protocolli decisionali e dal Codice Etico adottati unitamente al Modello nonché dall'insieme di regole, disposizioni organizzative, prassi, regolamenti, procedure operative del Sistema di Gestione Integrato Qualità/Ambiente/Sicurezza sui luoghi di lavoro e del Sistema di Responsabilità Sociale nonché di altri singoli Sistemi di Gestione, Codice Etico, Documento di Valutazione dei Rischi ex Decreto Legislativo n. 81/2008 che disciplinano e garantiscono il funzionamento della Società. Tale sistema coinvolge ogni settore dell'attività svolta dalla Società attraverso la distinzione dei compiti operativi da quelli di controllo, attutendo ragionevolmente ogni possibile conflitto di interesse.

Analoga *ratio* anima la previsione all'interno dello stesso Organismo di Vigilanza di sostituire il membro effettivo che si trovi in merito ad una determinata materia oggetto di vigilanza e controllo in potenziale conflitto di interessi.

L'originaria architettura dei controlli, sottoposta ad attenti e puntuali interventi di implementazione a seguito dell'adozione del Modello, è ora strutturata su un sistema basato sui seguenti elementi qualificanti:

- *in primis*, procedure mutate nei protocolli decisionali adottati unitamente al Modello approvato dal Consiglio di Amministrazione di ALLSYSTEM in data 26.02.2016 (e successivamente sottoposte a periodiche opere di implementazione e/o revisione);
- procedure e istruzioni operative predisposte nell'ambito del Sistema di Gestione Integrato Qualità/Ambiente/Salute e Sicurezza dei lavoratori e del Sistema di Responsabilità Sociale nonché nei singoli Sistemi di Gestione adottati in tema di sicurezza stradale sicurezza delle informazioni, continuità operativa, istituti di vigilanza privata e centri di monitoraggio e ricezioni allarme con la imprescindibile valutazione del rischio;
- controlli di monitoraggio sulla corretta attuazione delle istruzioni operative: attuato tramite meccanismi di autodiagnosi svolti periodicamente da parte della Direzione e dalle singole strutture aziendali preposte al controllo interno ovvero tramite periodica revisione esterna, esercitata da società consulenti terze e specializzate, finalizzata alla valutazione della conformità e dell'adeguatezza del sistema dei

controlli interni (procedure operative e regole) elaborati nell'ambito del Sistema di Gestione Integrato nonché negli altri singoli Sistemi di Gestione citati;

- sistemi e procedure contabili informatiche ispirate al principio della separazione/segregazione delle funzioni.

La ALLSYSTEM ha elaborato e adottato procedure operative nell'ambito di Sistemi di Gestione specifici e integrati, finalizzate a conformarsi alle seguenti normative riconosciute a livello internazionale:

- ISO 9001:2015 (Qualità), ISO 14001:2015 (Ambiente) e ISO 45001:2018 (Salute e Sicurezza dei Lavoratori) in relazione alle quali la Società si è dotata di un Sistema di Gestione Integrato;
- ISO 39001:2012 (Sicurezza Stradale);
- ISO 27001:2013 (Sicurezza delle Informazioni);
- ISO 22301:2019 (Continuità Operativa)
- UNI 10891:2022 (Istituti di Vigilanza Privata);
- UNI 50518:2020 (Centri di Monitoraggio e di Ricezione Allarme);
- SA8000:2012 (Responsabilità Sociale).

B3) L'aggiornamento del Modello.

L'aggiornamento a cui è stato sottoposto il presente Modello ha preso l'avvio dall'analisi dell'ormai consolidato sistema di controllo interno di ALLSYSTEM innanzi descritto, tenendo in espressa considerazione le indicazioni fornite in materia, ad oggi, dalle Autorità giudiziarie nei loro arresti giurisprudenziali.

Il processo di revisione e aggiornamento del Modello si è sviluppato, parimenti a quanto avvenuto in sede di elaborazione della prima versione del Modello stesso, in diverse fasi, basate sul rispetto dei principi di tracciabilità e verificabilità delle attività svolte dal *team* di lavoro istituito dalla Direzione societaria e composto da professionisti legali ed esperti nel processo di mappatura del rischio, sulla valutazione con l'elaborazione del *risk assessment*, limitatamente alle nuove fattispecie di reato presupposto introdotte o modificate a seguito dell'adozione del Modello, alla stesura dei relativi protocolli operativi, nonché alla revisione dei protocolli decisionali esistenti in ordine alle aree di attività di maggiore sensibilità e a rischio commissione reati rilevanti ai sensi del Decreto.

Nel corso dell'opera di elaborazione e di stesura della prima versione del Modello si era proceduto all'individuazione della mappa delle attività a rischio ovvero delle attività nel cui ambito possono essere commessi i reati e gli illeciti rilevanti (cfr. *infra* paragrafo 2.3.1), secondo quanto espressamente previsto dall'art. 6, c. 2, lett. a) del Decreto.

Tale analisi si è dunque resa nuovamente necessaria per la revisione/aggiornamento del Modello a seguito delle novelle legislative che hanno ampliato le fattispecie di reati presupposto nonché in ordine alle aree ritenute di maggiore sensibilità per la vita societaria.

Si era, poi, provveduto all'elaborazione di un codice etico (cfr. paragrafo 2.3.2) e di specifici protocolli di decisione, finalizzati a governare i profili di rischio enucleati a seguito dell'attività di mappatura delle attività societarie (cfr. paragrafo 2.3.3), secondo quanto richiesto dall'art. 6 c. 2 lett. b) del D.Lgs. 231/01, entrambi (codice etico e protocolli di decisione) oggetti dell'opera di rivalutazione necessitata dai *nova* intervenuti in seguito all'approvazione della prima versione del Modello.

In conformità a quanto richiesto dagli artt. 6 c. 2 lett. d) e lett. e) del Decreto, si era provveduto quindi alla strutturazione dell'Organismo di Vigilanza (così come riportato nel successivo capitolo 2), espressamente preposto al presidio dell'effettiva applicazione del Modello ed alla sua costante verifica in termini di adeguatezza ed efficacia; si era altresì delineato un apparato sanzionatorio (riportato nel successivo capitolo 3) avverso tutte le violazioni al Modello, divenute elementi integrativi delle condotte disciplinarmente significative previste dal CCNL dei dipendenti delle Aziende del Commercio applicabile in ALLSYSTEM; si erano poi stabilite le modalità di diffusione del Modello e di relativa formazione del personale (così come indicato nel successivo capitolo 4).

B4) La mappa delle attività a rischio del Modello adottato in data 26.02.2016.

La mappatura delle attività a rischio, che hanno preceduto l'adozione della prima versione del Modello, aveva preso avvio dall'analisi della documentazione disponibile e da approfondimenti tramite interviste ai responsabili di Direzione (consiglieri di amministrazione), ai responsabili delle varie funzioni aziendali, ai Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010, ai responsabili delle diverse filiali, all'estensore del DVR, all'RSPP e ad alcuni RLS (per un totale di oltre venti interviste) e tramite l'accesso nella sala conta di Torino, al fine di costruire un Modello il più possibile aderente agli specifici ambiti operativi e alla struttura organizzativa della società, con riferimento ai rischi di reato in concreto prospettabili.

Le interviste - finalizzate anche ad avviare il processo di sensibilizzazione rispetto alle previsioni di cui al D.Lgs. n. 231/2001 - erano state condotte con l'obiettivo di individuare i processi e le attività potenzialmente a rischio di commissione dei reati previsti dal Decreto nonché i presidi già esistenti atti a mitigare i predetti rischi.

Individuate tali aree, si era ritenuto opportuno procedere ad un accesso nella sala conta di importanti dimensioni di Torino, intervistando il *security manager* ed esaminando:

- tutta la contrattualistica in essere in relazione all'acquisto e alla manutenzione dei macchinari BCE *compliance* conta soldi;

- i verbali di ispezione della Banca di Italia, le risposte della Società e un'ulteriore intervista al Gruppo di Lavoro istituito dal Consiglio di Amministrazione con delibera del 31 luglio 2015 in esito alla ricezione del verbale ispettivo di Banca d'Italia del 14.7.2015;
- la nuova procedura adottata per superare i rilievi di Banca di Italia.

Si era assistito al procedimento di conferimento del denaro dai portavalori al *caveau*, di apertura dei plichi sotto una ferrea videosorveglianza, di contazione del denaro e di conferimento nel *caveau* con l'attribuzione ai singoli clienti; si era assistito anche al processo inverso, ovvero a quello della preparazione delle varie provviste in contanti per i clienti (bancomat, grande distribuzione etc.) che ne facciano richiesta un giorno per il successivo.

Si era proceduto altresì a riesaminare l'RSPP in contraddittorio con tre RLS delle filiali di Torino, Asti e Cuneo, unitamente all'ASPP di Torino, al fine di comprendere se l'area sicurezza sul lavoro fosse sufficientemente presidiata, chiedendo e ottenendo copiosa documentazione in materia di:

- libretto di viaggio degli automezzi;
- formazione delle guardie particolari giurate;
- funzionamento del software per la calendarizzazione della manutenzione dei mezzi;
- verbali di riunione RSPP/RLS;
- sanzioni disciplinari;
- registri infortuni singole filiali.

Era stata così effettuata una mappatura di tutta l'attività della Società, articolata sulla base dei processi e delle attività svolte da ciascuna Direzione/Funzione aziendale, con evidenza dello specifico profilo di rischio e del sistema di controlli esistente a prevenire i comportamenti illeciti, individuando gli interventi di miglioramento necessari per superare le carenze riscontrate e riportate nella *gap analysis*.

I risultati di tale attività erano stati formalizzati in memoranda degli incontri con le singole Direzioni/Funzioni e in un documento denominato "Mappa dei rischi 231" e sottoposti all'esame dei responsabili intervistati.

Tali documenti sono stati messi a disposizione dell'Organismo di Vigilanza ai fini dello svolgimento dell'attività istituzionale ad esso demandata.

Conformemente a quanto previsto dall'art. 6, comma 2, lett. a) D.Lgs. 231/01 si riportano le aree di attività aziendali individuate originariamente come a rischio, ovvero nel cui ambito

potrebbero essere presenti rischi potenziali di commissione delle fattispecie di reato previste dal Decreto.

In particolare erano state identificate le seguenti aree di rischio:

- spendita e contazione denaro falsificato;
- riciclaggio;
- sicurezza sul lavoro con particolare riferimento al tema della formazione del personale dipendente;
- gestione delle attività commerciali in generale ed in particolare delle gare con enti pubblici o a partecipazione pubblica;
- rapporti, adempimenti verso la Pubblica Amministrazione e visite ispettive;
- gestione dei flussi finanziari;
- operazioni straordinarie e di M&A;
- selezione, assunzione e gestione del personale;
- contabilità e bilancio (tenuta della contabilità, predisposizione del Bilancio e gestione delle operazioni straordinarie).

In tali aree/processi si sono ritenuti maggiormente rilevanti i rischi di commissione di alcune fattispecie di reato indicate negli artt. 25 (reati contro la Pubblica Amministrazione), 25 *bis* (falsità in monete), 25 *septies* (lesioni e omicidio colposo in violazione della normativa in materia di sicurezza sul lavoro), 25 *octies* (ricettazione, riciclaggio e auto riciclaggio) di cui al Decreto.

Relativamente agli altri reati ed illeciti (e tipicamente i reati di falsità in strumenti o segni di riconoscimento, quelli in materia di pratiche di mutilazione degli organi genitali femminili, quelli con finalità di terrorismo o di eversione dell'ordine democratico, i reati ed illeciti amministrativi di abuso di mercato, i delitti in materia di diritto d'autore, i delitti contro l'industria e il commercio, i delitti contro la personalità individuale ed i reati transnazionali) si è ritenuto che la specifica attività svolta dalla Società non presenti profili di rischio tali da rendere ragionevolmente fondata la possibilità della loro commissione nell'interesse o a vantaggio della stessa. Si è pertanto stimato esaustivo il richiamo ai principi contenuti sia nel presente Modello che nel Codice Etico, ove si vincolano gli esponenti aziendali, i collaboratori ed i *partners* commerciali al rispetto dei valori di tutela della personalità individuale, correttezza, moralità e rispetto delle leggi.

B5) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2019

La mappatura delle attività a rischio in sede di aggiornamento del modello – reso necessario dall'introduzione *medio tempore* di ulteriori fattispecie di illeciti presupposto, tra cui a titolo d'esempio, l'istigazione alla corruzione tra privati (introdotto all'art. 2635 *bis* c.c. dal D.Lgs. 15 marzo 2017, n. 38 e inserito nel novero dei reati presupposto alla lettera *s bis*) dell'art. 25

ter del Decreto, unitamente al già compendiato art. 2635 c.c.), l'intermediazione illecita o sfruttamento del lavoro – (reato introdotto all'art. 603 bis c.p. dalla L. 29 ottobre 2016, n. 199 e parimenti inserito nel novero dei reati presupposto all'art. 25 *quinquies*, comma 1, lett a) del Decreto) – e di rivisita parziale dei protocolli nel 2019 ha preso avvio dall'analisi della documentazione formata a seguito dell'adozione del Modello vigente. Sono stati messi a disposizione, oltre al Modello adottato e ai relativi allegati:

- funzionigramma/organigramma di ALLSYSTEM aggiornato;
- visura C.C.I.A.A. di ALLSYSTEM aggiornata;
- verbali redatti dall'O.D.V. Monocratico;
- segnalazioni pervenute all'O.D.V. Monocratico (annualità 2016, 2017, 2018, 2019);
- verbali organi ispettivi e registro annotazioni visite ispettive;
- D.V.R. aggiornato, comprensivo di 31 schede elaborate in relazione ai rischi per la sicurezza e per la salute presenti nelle singole aree/mansioni prese in considerazione;
- verbali delle riunioni periodiche ai sensi dell'art. 35 D.Lgs. n. 81/2008;
- piani di emergenza ed evacuazione e prove evacuazione per ogni singola Filiale di ALLSYSTEM;
- estratto libri infortuni di ciascuna sede/filiale di ALLSYSTEM e tabelle analisi infortuni così suddivise: complessive per le annualità 2016, 2017 e 2018; per sedi e filiali per le annualità 2016, 2017 e 2018; analisi infortuni per triennio;
- procedimenti disciplinari instaurati nelle filiali di Asti e Torino nei confronti dei dipendenti di ALLSYSTEM.

A seguito dell'analisi della documentazione suelencata, si è ritenuto di dover procedere ad approfondimenti ulteriori provvedendo a nuove interviste delle figure chiave nelle aree ritenute di interesse.

B6) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2020

La mappatura delle attività a rischio in sede di aggiornamento del modello nell'anno 2020 e la conseguente predisposizione di un nuovo protocollo decisionale si è resa necessaria in ragione della recente introduzione nel novero degli illeciti presupposto di gran parte dei reati tributari disciplinati dal D.Lgs. n. 74/2000, di quelli di contrabbando e del delitto di frode in pubbliche forniture ad opera delle novelle legislative apportate dal D.L. 26 ottobre 2019 n. 124 (convertito con modificazioni nella L. 19 dicembre 2019 n. 157) e dal D.Lgs. 14 luglio 2020 n. 75.

Il compimento della summenzionata attività si è reso possibile a fronte dell'analisi della documentazione formata a seguito dell'adozione del Modello vigente. La Società ha quindi messo a disposizione, oltre al Modello adottato e ai relativi allegati:

- funzionigramma/organigramma di ALLSYSTEM aggiornato;
- visura C.C.I.A.A. di ALLSYSTEM aggiornata;
- verbali redatti dall'O.D.V. Monocratico (annualità 2019-2020);
- segnalazioni pervenute all'O.D.V. Monocratico (annualità 2019 e 2020);
- atto di cessione del ramo d'azienda stipulato in data 23.06.2020 tra ALLSYSTEM (cedente) e Vedetta 2 Mondialpol S.p.A. (cessionaria);
- contestazioni ITL e SPRESAL;
- albo fornitori e albo clienti aggiornati ad ottobre 2020;
- atti relativi all'acquisto da parte di ALLSYSTEM dell'immobile di Torino, via E. FERMI n. 8 e successiva vendita a AllSystem1 S.r.l.;
- documentazione attinente la verifica fiscale del 2016 ad opera della GDF di Biella in relazione all'a.i. 2014, successivo avviso di accertamento dell'A.E. di Torino e definizione mediante ravvedimento operoso;

A seguito dell'analisi della documentazione suelencata, si è ritenuto di dover procedere ad approfondimenti ulteriori provvedendo a nuove interviste delle figure chiave nelle aree ritenute di interesse.

All'esito di quanto emerso nel corso delle interviste, la Società ha provveduto a mettere a disposizione l'ulteriore documentazione di seguito compendiate:

- comunicazioni relative alle procedure interne adottate dalla Società nell'ambito dell'approvvigionamento di beni/servizi e modalità di contabilizzazione della documentazione fiscale;
- contratto di conservazione dei documenti informatici su piattaforma cloud stipulato con TeamSystem Service S.r.l.;
- rinnovo contratto assistenza e manutenzione prodotto Archivia V3 per l'anno 2020 fornita da Omicron Consulting S.r.l.;
- contratto di rete di imprese tra AllSystem S.p.a., AllSystem1 S.r.l. e Tecnel Impianti S.r.l.;

- accordo transattivo raggiunto nel dicembre 2016 tra Regione Piemonte e il R.T.I., all'interno del quale era ricompresa anche ALLSYSTEM, esecutrici di un contratto di appalto relativo al servizio di vigilanza presso gli immobili regionali siti nella provincia di Torino.

B7) La mappa delle attività a rischio in fase di aggiornamento del Modello nel 2023

La mappatura delle attività a rischio in sede di aggiornamento del modello nell'anno 2023 e la conseguente predisposizione di nuovi protocolli decisionali si è resa necessaria in ragione della fusione per incorporazione di ALLSYSTEM1 S.r.l. in ALLSYSTEM S.p.a., del venire meno di parte delle attività compiute sino al giugno 2020 (trasporto e contazione valori) nonché della introduzione nel novero degli illeciti presupposto di ulteriori fattispecie di reato quali:

- i delitti di turbata libertà degli incanti e di turbata libertà del procedimento di scelta del contraente ad opera del D.L. 10.08.2023 n. 105 (convertito con modificazioni dalla L. 9.10.2023 n. 137);
- i delitti contro il patrimonio culturale e i delitti di riciclaggio di beni culturali e devastazione e saccheggio di beni culturali e paesaggistici ad opera della L. 9 marzo 2022 n. 22;
- i delitti in materia di strumenti di pagamento diversi dai contanti e in materia di trasferimento fraudolento di valori ad opera del D.Lgs. 8 novembre 2021 n. 184 nonché del D.L. 10 agosto 2023 n. 105 (convertito con modificazioni dalla L. 9.10.2023 n. 137).

A ciò si aggiungano anche le modifiche legislative che hanno interessato, attraverso l'ampliamento della descrizione delle condotte punite, reati già inclusi nel novero degli illeciti presupposto (in relazione ai quali erano stati adottati specifici protocolli) ed in particolare quelli di cui:

- agli artt. 615-*quater*, 615-*quinquies* e 617-*quinquies* c.p. ad opera della L. 23 dicembre 2021 n. 38 che ha recepito e dato attuazione alla Direttiva UE 2013/40 in tema di attacchi ai sistemi informatici;
- all'art. 640-*ter* c.p. ad opera del D.Lgs. 8 novembre 2021 n. 184 che ha recepito e dato attuazione Direttiva UE 2019/713 relativa alla lotta contro le frodi e le falsificazioni di mezzi di pagamento diversi dai contanti;
- agli artt. 648, 648-*bis*, 648-*ter* e 648-*ter*1 c.p. ad opera del D.Lgs. 8 novembre 2021 n. 195 che ha recepito e dato attuazione alla Direttiva UE 2018/1673 in tema di lotta al riciclaggio mediante il diritto penale.

In ultimo, la suddetta attività di implementazione del Modello si è resa necessaria anche a seguito di vicende giudiziarie che hanno interessato società operanti nel settore della vigilanza privata - con specifico riferimento alla vigilanza non armata, ovvero quella relativa ai c.d. operatori fiduciari) - ove la Procura di Milano ha mosso la contestazione provvisoria

del reato di cui all'art. 603-bis c.p. (c.d. caporalato) avendo ipotizzato lo sfruttamento dello stato di bisogno dei soli lavoratori sopra indicati, pur a fronte dell'osservanza delle indicazioni provenienti dai CCNL di categoria che si sono susseguiti nel tempo e, nello specifico, pur a fronte della rigorosa applicazione delle retribuzioni ivi determinate.

Il compimento della summenzionata attività si è reso possibile a fronte dell'analisi della documentazione formata a seguito dell'adozione del Modello vigente. La Società ha quindi messo a disposizione, oltre al Modello adottato ed ai relativi allegati:

- funzionigramma/organigramma di ALLSYSTEM aggiornato;
- visura C.C.I.A.A. di ALLSYSTEM aggiornata;
- verbali redatti dall'O.d.V. Monocratico e segnalazioni pervenute al medesimo (annualità 2021-2023);
- atto di fusione per incorporazione nella ALLSYSTEM S.p.a. della ALLSYSTEM 1 S.r.l. nonché di scissione parziale della ALLSYSTEM S.p.a. a favore della ALLSYSTEM 3 S.r.l. del 13.03.2023;
- DVR aggiornato in data 11.04.2023 a seguito delle modifiche organizzative conseguenti all'incorporazione della ALLSYSTEM 1 S.r.l. nella ALLSYSTEM S.p.a. nonché le schede M29, M30 e M31 relative alla nuova attività di installazione e manutenzione di sistemi di allarme e sicurezza svolta a seguito della suddetta operazione straordinaria;
- registro infortuni di ALLSYSTEM S.p.a. aggiornato;
- registro infortuni di ALLSYSTEM 1 S.r.l. compilato dal 2018 al 2023 e n. 12 denunce infortuni presentate dal 2019 al 2023;
- contratti di appalto stipulati aventi ad oggetto servizi di vigilanza prestati in favore di enti museali;
- sanzioni disciplinari di maggiore rilievo elevate nei confronti di dipendenti di ALLSYSTEM S.p.a.
- visite ispettive ad opera dell'INL, Questura e SPreSAL ed esiti dei relativi accertamenti;

A seguito dell'analisi della documentazione suelencata, si è proceduto ad approfondimenti ulteriori attraverso interviste delle figure chiave nelle aree ritenute di interesse.

All'esito di quanto emerso nel corso delle interviste, la Società ha provveduto a mettere a disposizione l'ulteriore documentazione di seguito compendiate:

- Relazioni periodiche trimestrali del RSPP (dal I trimestre 2021 al I trimestre 2023) con relativi esiti delle ispezioni e le verifiche effettuate presso le Filiali di AllSystem ed dei sopralluoghi presso i clienti.

B8) Il Codice Etico.

Per quanto concerne le norme etico comportamentali, la Società ha adottato un Codice Etico (Allegato 2), improntato alle esigenze espresse dal D.Lgs. 231/2001 ed ispirato alla sana, trasparente e corretta gestione della Società, che completa e integra il sistema dei poteri e i principi generali di controllo interno dell'azienda, inclusi i protocolli di decisione di cui al successivo paragrafo.

Il Codice Etico rende espliciti i fondamenti della propria cultura aziendale e i valori di riferimento dai quali fa derivare regole concrete di comportamento verso tutti i soggetti interni ed esterni, che hanno direttamente o indirettamente una relazione con ALLSYSTEM: i clienti, i soci e i collaboratori in primo luogo, ma anche i fornitori, i partner commerciali, gli enti pubblici e a partecipazione pubblica, i committenti in senso lato e l'ambiente in cui la Società opera.

B9) I protocolli di decisione.

L'analisi delle attività a rischio e del relativo sistema di controllo ha condotto all'elaborazione di specifici protocolli (riportati in Allegato 4), in conformità a quanto prescritto dall'art. 6 c. 2 lett. b) D.Lgs. 231/01, che contengono un insieme di regole e di principi di controllo ritenuti idonei a governare il profilo di rischio individuato.

In particolare, per ciascuna area a rischio è stato creato un protocollo in cui si rilevano:

- gli obiettivi del documento;
- l'ambito di applicazione e le eventuali procedure aziendali di riferimento;
- i ruoli e le responsabilità degli attori coinvolti nel processo;
- la descrizione sintetica del processo;
- i principi di comportamento;
- i principi di controllo;
- i flussi informativi verso l'Organismo di Vigilanza;
- la diffusione e manutenzione del protocollo.

I principi di controllo riportati nei protocolli fanno riferimento a:

- i livelli autorizzativi chiari e definiti sulla base del sistema dei poteri adottato;
- la separazione funzionale delle attività operative e di controllo;
- i controlli specifici di quadratura, verifiche di conformità, adeguatezza;

- la verificabilità e la documentabilità delle operazioni a rischio e dei controlli posti in essere per prevenire i comportamenti illeciti.

I protocolli sono stati sottoposti all'esame dei responsabili delle Direzioni garanti della gestione delle attività e dei processi a rischio, al fine di ottenere la loro valutazione ed approvazione, implementando in tal modo regole efficaci ed idonee alla prevenzione in concreto delle ipotesi di rischio riscontrate.

Particolare attenzione è stata inoltre dedicata ad individuare e regolare i processi di gestione e di controllo delle risorse finanziarie nelle attività ritenute a rischio della realizzazione degli illeciti rilevanti ai sensi del Decreto, nel rispetto dei principi di trasparenza, verificabilità, inerenza all'attività aziendale.

I protocolli richiamano ed integrano i principi contenuti nel Codice Etico, nelle procedure del Sistema Qualità, in particolare quelle identificate come rilevanti ai sensi del D.Lgs. 231/2001, nel Documento di Valutazione del Rischio e nel sistema dei poteri e nelle regole adottate di controllo interno.

Laddove ritenuto opportuno, si provvederà alla emanazione di apposite procedure interne che recepiscano nel dettaglio le singole disposizioni.

B10) L'Organismo di Vigilanza.

B10 – I) Caratteristiche dell'Organismo di Vigilanza.

Ai sensi del Decreto, il compito di vigilare sul funzionamento, l'efficacia e l'osservanza del Modello, nonché di curarne l'aggiornamento deve essere affidato ad un organismo interno all'Ente dotato di autonomi poteri di iniziativa e di controllo (l'"Organismo di Vigilanza").

Le attribuzioni ed i poteri dell'Organismo di Vigilanza (di seguito, anche l'"Organismo") sono stati conferiti in ALLSYSTEM ad un organo monocratico nominato dal Consiglio di Amministrazione e avente caratteristiche di autonomia, indipendenza, professionalità necessarie per il corretto ed efficiente svolgimento delle funzioni ad esso assegnate.

L'Organismo di Vigilanza è dotato di poteri di iniziativa e di controllo sulle attività della società, senza disporre di poteri gestionali e/o amministrativi. Inoltre, onde poter svolgere, in assoluta indipendenza, le proprie funzioni, dispone di autonomi poteri di spesa.

L'Organismo di Vigilanza si avvale ordinariamente delle varie funzioni aziendali per l'espletamento dei suoi compiti di vigilanza e controllo.

Laddove ne ravvisi la necessità, in funzione della specificità degli argomenti trattati, può inoltre avvalersi di consulenti esterni che individua in professionalità specifiche e qualificate.

Per quanto concerne in particolare la materia della tutela della salute e della sicurezza sul luogo di lavoro, l'Organismo potrà avvalersi di tutte le risorse attivate per la gestione dei relativi aspetti (Responsabile del Servizio Prevenzione e Protezione, Rappresentante dei lavoratori per la sicurezza, Medico competente, ecc.) e, più in generale, di quelle previste dalle normative di settore, *in primis* dal D. Lgs. n. 81/2008.

L'Organismo di Vigilanza, direttamente o per il tramite delle varie funzioni aziendali all'uopo designate, ha accesso a tutte le attività svolte dalla Società e alla relativa documentazione.

B10 – II) Composizione, durata e compensi dell'Organismo di Vigilanza.

L'Organismo di Vigilanza è composto da un membro effettivo.

Al fine di assicurare l'operatività dell'Organismo di Vigilanza anche nei casi di sospensione ovvero di temporaneo impedimento del suo componente, il Consiglio di Amministrazione nomina altresì un componente supplente.

L'Organismo di Vigilanza resta in carica per la durata stabilita dal Consiglio di Amministrazione all'atto della nomina; in assenza di una specifica determinazione, l'Organismo di Vigilanza dura in carica per tutto il periodo in cui resta in carica il Consiglio di Amministrazione che lo ha nominato.

La revoca del componente - fatti salvi i casi infra previsti - può avvenire unicamente nel caso di rilevanti inadempimenti nell'assolvimento dei suoi compiti.

L'Organismo di Vigilanza si intende decaduto se viene a mancare, per dimissioni o decadenza, il suo componente. In tal caso il Consiglio di Amministrazione provvede tempestivamente a nominare il nuovo membro, prevedendo la sostituzione *ad interim* con il membro supplente.

Il Consiglio di Amministrazione delibera il compenso spettante al componente dell'Organismo di Vigilanza per lo svolgimento delle relative funzioni, stabilendo altresì il compenso spettante al membro supplente dell'Organismo stesso, sotto forma di emolumento fisso in ragione della necessità del suo intervento in luogo del componente effettivo.

Ai membri – effettivo e supplente – compete altresì il rimborso delle spese vive e documentate sostenute per l'espletamento delle funzioni.

B10 – III) Requisiti di eleggibilità, cause di decadenza e sospensione. Requisiti di onorabilità.

La nomina quale componente dell'Organismo di Vigilanza è condizionata alla presenza di requisiti soggettivi di eleggibilità.

Nella scelta dei componenti gli unici criteri rilevanti sono quelli che attengono alla specifica professionalità e competenza richiesta per lo svolgimento delle funzioni dell'Organismo, all'onorabilità ed all'assoluta autonomia ed indipendenza rispetto alla Società.

■ **Requisiti soggettivi di onorabilità ai fini dell'eleggibilità dell'Organismo di Vigilanza.**

Quanto ai requisiti di onorabilità, la carica di componente dell'Organismo di Vigilanza non può essere assunta da coloro che:

- a) si trovano in una delle condizioni di ineleggibilità o decadenza previste dall'articolo 2382 c.c.;
- b) sono stati sottoposti a misure di prevenzione disposte dall'autorità giudiziaria ai sensi del D. Lgs. 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione) e successive modificazioni ed integrazioni, salvi gli effetti della riabilitazione;
- c) sono stati condannati con sentenza irrevocabile, salvi gli effetti della riabilitazione:
 1. alla reclusione per uno dei reati previsti nel Titolo XI del Libro V del codice civile e nel Regio Decreto del 16 marzo 1942, n. 267 (Legge Fallimentare) nonché del Decreto Legislativo 12 gennaio 2019, n. 14 (Codice della crisi d'impresa e dell'insolvenza);
 2. alla reclusione o all'arresto per un tempo non inferiore a un anno per un delitto contro la pubblica amministrazione, contro la fede pubblica, il patrimonio, l'ordine pubblico, l'economia pubblica, illeciti ambientali ovvero delitti in materia tributaria;
 3. alla reclusione per un tempo non inferiore a due anni per un qualunque delitto non colposo.

La carica di componente dell'Organismo non può essere ricoperta da coloro ai quali sia stata applicata su richiesta delle parti ex art. 444 c.p.p. una delle pene previste indicate alla lettera c) del precedente paragrafo, salvo il caso dell'estinzione del reato a seguito di accertamento giudiziale in sede esecutiva.

- d) siano stati condannati, con sentenza irrevocabile o con sentenza non definitiva anche se a pena condizionalmente sospesa, fatti salvi gli effetti della riabilitazione, per uno degli illeciti per i quali è applicabile il Decreto n. 231/2001. Per sentenza di condanna si intende anche quella pronunciata ai sensi dell'art. 444 c.p.p. salvo il caso di estinzione del reato a seguito di accertamento giudiziale in sede esecutiva;
- e) abbiano rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, anche con provvedimento non definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica.

I soggetti che si trovino in una delle suddette situazioni non possono essere nominati e se nominati decadono automaticamente dall'incarico.

L'Organismo di Vigilanza certifica, mediante dichiarazione sottoscritta e rilasciata dal designato componente entro 30 giorni dalla nomina, la sussistenza in capo al medesimo dei requisiti prescritti. Tale dichiarazione viene trasmessa dall'O.d.V. al Consiglio di Amministrazione.

L'infedele dichiarazione da parte del componente dell'O.d.V. ne comporta l'immediata decadenza.

■ Cause di decadenza

Il componente dell'Organismo di Vigilanza, successivamente alla nomina, decade da tale carica, qualora:

- si accerti che ha rivestito la qualifica di componente dell'Organismo di Vigilanza in seno a società nei cui confronti siano state applicate, con provvedimento definitivo (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
- sia stato condannato, con sentenza definitiva (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.), anche se a pena sospesa condizionalmente per uno degli illeciti tra quelli per i quali è applicabile il Decreto n. 231/2001;
- il componente dell'O.d.V. decade automaticamente qualora si dovesse realizzare una delle cause di cui alle lettere a), b) e c) numeri 1, 2 e 3 di cui al precedente paragrafo, nonché alle lettere d) ed e) del medesimo.

Il componente dell'Organismo di Vigilanza deve comunicare al Presidente del Consiglio di Amministrazione, sotto la sua piena responsabilità, il sopravvenire di una delle cause sopra elencate di decadenza.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una causa di decadenza, convoca senza indugio il Consiglio di Amministrazione affinché proceda – nella sua prima riunione successiva all'avvenuta conoscenza – alla dichiarazione di decadenza dell'interessato dalla carica di componente dell'Organismo di Vigilanza ed alla sua immediata sostituzione.

■ Cause di sospensione

Costituiscono cause di sospensione dalla funzione di componente dell'Organismo di Vigilanza le seguenti circostanze:

1. si accerti, 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 (compresa la sentenza emessa ai sensi dell'art. 63 del Decreto ancora non passata in giudicato), le sanzioni previste dall'art. 9 del medesimo Decreto, per illeciti commessi durante la loro carica;
2. i componenti dell'Organismo di Vigilanza siano stati condannati con sentenza non definitiva, anche a pena sospesa condizionalmente (intendendosi per sentenza di condanna anche quella pronunciata ai sensi dell'art. 444 c.p.p.) per uno degli illeciti tra quelli per i quali è applicabile il Decreto n. 231/2001;
3. l'avvenuta condanna con sentenza non definitiva per uno degli illeciti di cui al precedente paragrafo in tema di requisiti di onorabilità e nei limiti di pena ivi previsti;

4. l'applicazione provvisoria di una delle misure previste dall'articolo 67, comma 3, del D. Lgs. 6 settembre 2011, n. 159 (Codice delle leggi antimafia e delle misure di prevenzione), e successive modificazioni e integrazioni;
5. l'applicazione di una misura cautelare di tipo personale.

Il Consiglio di Amministrazione iscrive l'eventuale revoca dei soggetti, dei quali ha dichiarato la sospensione, fra le materie da trattare nella prima seduta consiliare successiva al verificarsi di una delle cause di sospensione indicate. Nelle ipotesi previste sub 4) e 5), la sospensione si applica in ogni caso per l'intera durata delle misure ivi previste.

In tali casi il Consiglio di Amministrazione dispone la sospensione della qualifica di componente l'Organismo di Vigilanza e senza indugio provvede alla nomina di un nuovo membro.

I componenti dell'Organismo di Vigilanza debbono comunicare al Presidente del Consiglio di Amministrazione, sotto la loro piena responsabilità, il sopravvenire di una delle cause di sospensione di cui sopra.

Il Presidente del Consiglio di Amministrazione, anche in tutti gli ulteriori casi in cui venga direttamente a conoscenza del verificarsi di una delle cause di sospensione dianzi citate, convoca senza indugio il Consiglio di Amministrazione affinché provveda, nella sua prima riunione successiva, a dichiarare la sospensione del soggetto nei cui confronti si è verificata una delle cause di cui sopra dalla carica di componente dell'Organismo di Vigilanza ed alla sua sostituzione.

B10 – IV) Compiti dell'Organismo di Vigilanza.

L'Organismo di Vigilanza, nell'esecuzione della sua attività ordinaria, vigila in generale:

- 1) sul funzionamento, sull'efficienza, efficacia ed adeguatezza del Modello nel prevenire e contrastare la commissione degli illeciti per i quali è applicabile il D. Lgs. n. 231/2001;
- 2) sull'osservanza delle prescrizioni contenute nel Modello da parte dei destinatari, rilevando la coerenza e gli eventuali scostamenti dei comportamenti attuati, attraverso l'analisi dei flussi informativi e le segnalazioni alle quali sono tenuti i responsabili delle varie funzioni aziendali;
- 3) sull'aggiornamento del Modello, del Codice Etico e del procedimento di mappatura del rischio ai fini della individuazione di nuove aree sensibili, formulando proposte agli Organi Societari competenti, laddove si riscontrino esigenze di adeguamento ovvero si rendano opportune o necessarie (anche ai sensi dell'art. 30, quarto comma, D.Lgs. n. 81/2008) modifiche e/o integrazioni in conseguenza di significative violazioni delle prescrizioni del Modello stesso, significativi mutamenti dell'assetto

organizzativo e procedurale della società, nonché novità legislative in materia quali, a titolo esemplificativo, l'introduzione di nuovi illeciti presupposto;

- 4) sull'attuazione e aggiornamento del piano di formazione del personale proprio in materia di presupposti della responsabilità amministrativa e di eventuali nuovi illeciti presupposto;
- 5) sul puntuale adempimento dell'obbligo di informazione nei confronti dell'Organismo da parte delle funzioni aziendali a ciò chiamate ex art. 6, comma 2, lett. d) del Decreto;
- 6) sull'avvio e sullo svolgimento del procedimento di irrogazione di un'eventuale sanzione disciplinare a seguito dell'accertata violazione del Modello e del Codice Etico da parte di propri dipendenti e/o apicali ex art. 6, comma 2, lett. e) del Decreto;
- 7) sulle segnalazioni di condotte illecite rilevanti ai sensi del Decreto nonché di violazioni del Modello allo stesso pervenute ai sensi dell'art. 6, comma 2 *bis* del Decreto medesimo, disposizione modificata dal D.Lgs. 10 marzo 2023 n. 24 (c.d. Decreto Whistleblowing) attuativo della Direttiva UE 2019/1937 del Parlamento Europeo e del Consiglio del 23 ottobre 2019.

B10 – V) Modalità e periodicità di riporto agli Organi Societari.

L'Organismo di Vigilanza in ogni circostanza in cui sia ritenuto necessario o opportuno, ovvero se richiesto, riferisce al Consiglio di Amministrazione circa il funzionamento del Modello, l'osservanza del Codice Etico, l'esito della sua attività di vigilanza di cui al paragrafo precedente e l'adempimento agli obblighi imposti dal Decreto.

L'Organismo di Vigilanza, su base semestrale, trasmette al Consiglio di Amministrazione una specifica informativa sull'adeguatezza e sull'osservanza del Modello, che ha ad oggetto:

- 1) l'attività svolta;
- 2) le risultanze dell'attività svolta;
- 3) gli interventi correttivi e migliorativi pianificati ed il loro stato di realizzazione;
- 4) più in generale, l'esito dell'attività di vigilanza;
- 5) l'esito della sua attivazione a fronte della ricezione delle segnalazioni anche anonime o, comunque, mediante canali che siano in grado di garantire la riservatezza dell'identità del soggetto segnalante.

B10 – VI) Flussi informativi verso l’Organismo di Vigilanza.

Flussi informativi da effettuarsi al verificarsi di particolari eventi.

l) L’art. 6, comma 2, lett. d) del Decreto dispone che il Modello deve prevedere “*obblighi di informazione nei confronti dell’O.d.V.*”, affinché tale Organismo possa espletare correttamente la propria funzione.

A questo proposito il comma 2 *bis* dell’art. 6 del Decreto, introdotto dalla L. 30 novembre 2017, n. 179, disponeva che il Modello dovesse prevedere:

“a) uno o più canali che consentano ai soggetti indicati nell’articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell’integrità dell’ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell’ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell’identità del segnalante nelle attività di gestione della segnalazione;
b) almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell’identità del segnalante;
c) il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;
d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate”.

Nella nuova versione conseguente alla novella del 2023 il comma 2 *bis* dell’art. 6 del Decreto ribadisce la necessità di codificare canali interni di segnalazione che consentano al Gestore del canale di segnalazione (d’ora in avanti, per brevità, anche Gestore) nonché all’Organismo di Vigilanza di venire a conoscenza rispettivamente di violazioni rilevanti ai sensi del D. Lgs. n. 24/2023 e di violazioni del Modello, del Codice Etico ovvero di condotte concretanti illeciti presupposto di cui al D. Lgs. n. 231/2001.

L’individuazione del Gestore del canale di segnalazione deve ricadere ai sensi dell’art. 4 comma 2 D. Lgs. n. 24 del 2023 su un soggetto o un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del suddetto canale, ovvero su un soggetto esterno, anch’esso autonomo e con personale specificamente formato.

Il Gestore è quindi abilitato a gestire in prima battuta la segnalazione delle violazioni e a trattare in prima persona esclusivamente le violazioni sensibili ai sensi del D. Lgs. n. 24/2023.

Nel caso in cui la violazione segnalata concerna, invece, tematiche sensibili ai fini del Decreto n. 231/2001 (ovvero illeciti presupposto, infrazioni del Modello, delle procedure dal medesimo richiamate nonché del Codice Etico) il Gestore dovrà condividere senza ritardo

tali segnalazioni con l'Organismo di Vigilanza per le attivazioni di competenza di quest'ultimo. In tali casi dovrà dunque essere attivato un flusso ad evento tra Gestore ed Organismo di Vigilanza.

Deve quindi essere garantita da apposita Procedura aziendale la tempestiva informativa da parte di tutti i Destinatari (vale a dire da Amministratori, Soci, Dipendenti, Consulenti e/o Collaboratori nonché Organi della Società ed eventuali altri soggetti indicati nella Procedura *Whistleblowing*), relativa a qualsiasi violazione - anche solo 'tentata', cioè condotte che si siano arrestate alla soglia del tentativo - dei principi / protocolli contenuti nel Codice Etico, nel Modello ovvero di condotte concretanti illecito presupposto.

La Società ha a tal fine adottato una specifica Procedura di Whistleblowing (alla quale si rinvia), quale parte integrante del presente Modello, che garantisce l'immediata acquisizione della segnalazione da parte del Gestore e, nel caso in cui la violazione segnalata concerna tematiche sensibili ai fini 231/2001, la condivisione senza ritardo della medesima con l'Organismo di Vigilanza.

I Destinatari, in particolare, devono segnalare all'O.d.V. per il tramite del canale interno di segnalazione, le notizie relative alla commissione o alla potenziale commissione di illeciti o di comportamenti non conformi ai principi ed alle prescrizioni contenuti nel Modello, come meglio individuati nella Procedura *Whistleblowing*.

In particolare devono essere obbligatoriamente trasmesse, senza ritardo e comunque entro tre giorni lavorativi dalla compiuta conoscenza, all'Organismo di Vigilanza tramite la Procedura *Whistleblowing* le informazioni, il più possibile circostanziate (l'elencazione che segue è puramente esemplificativa e non esaustiva), relative:

- 1) alla commissione, o alla ragionevole convinzione di commissione, degli illeciti per i quali è applicabile il D. Lgs. n. 231/2001, compreso l'avvio di procedimento giudiziario a carico di qualsiasi dipendente/consulente/apicale operante nell'interesse della Società per reati previsti nel D. Lgs. n. 231/2001 e ciò a prescindere dal contestuale avvio di un procedimento per responsabilità amministrativa a carico della Società;
- 2) alla commissione o alla potenziale commissione di violazioni del Modello (Parte Generale e/o Parte Speciale), del Codice Etico e/o delle procedure aziendali (ivi compresa la Procedura *Whistleblowing*);
- 3) a eventuali ordini impartiti da soggetti gerarchicamente superiori e ritenuti dal segnalante in contrasto con la legge, le procedure aziendali, il Codice Etico e/o il Modello;
- 4) a eventuali richieste o offerte di denaro, di doni o di altre utilità provenienti da o destinate a pubblici ufficiali, incaricati di pubblico servizio e, comunque, soggetti appartenenti o collegati alla P.A.;

- 5) a eventuali induzioni, provenienti da un pubblico ufficiale o incaricato di un pubblico servizio e, comunque, da soggetti appartenenti o operanti per la P.A., a dare o promettere indebitamente al medesimo o ad un terzo denaro o altre utilità;
- 6) a eventuali offerte di denaro (o altre utilità) non dovute, provenienti o promesse da soggetti operanti nella (o per la) Società e rivolte agli apicali (amministratori, direttori generali, dirigenti, sindaci, liquidatori) di altra Società, Associazione o Ente privato;
- 7) a eventuali omissioni, trascuratezze o falsificazioni [sia 'materiali' (da intendersi come manomissioni/correzioni indebite del documento oggetto di falsificazione) sia ideologiche (da intendersi, ad esempio, come formalizzazione dell'operazione in fattura tra soggetti diversi da quelli che effettivamente hanno preso parte all'operazione o per ammontare diverso da quello reale)] nella tenuta della contabilità o nella conservazione della documentazione su cui si fondano le registrazioni contabili;
- 8) a notizie ufficiali provenienti da organi di Polizia Giudiziaria o da qualsiasi altra Autorità dalle quali si evinca anche il semplice svolgimento di indagini che interessano, anche indirettamente, la Società, il suo personale ed i componenti dagli Organi della Società;
- 9) a eventuali ispezioni, accessi, contestazioni, rilievi, verbali di Autorità di Vigilanza, Ispettive, Pubblica Sicurezza, Polizia Giudiziaria, etc. relative a potenziali violazioni riferibili a personale operante per la Società; le notizie relative alla commissione, o alla ragionevole convinzione di commissione, degli illeciti in materia di tutela della sicurezza e della salute sul lavoro compreso l'avvio di procedimento giudiziario e/o amministrativo a carico di qualsiasi dipendente/consulente/apicale operante nell'interesse della Società per le violazioni della normativa in materia di salute e sicurezza sul lavoro e ciò a prescindere dal contestuale avvio di un procedimento per responsabilità amministrativa a carico della Società;

Oltre alla doverosa informativa all'Organismo di Vigilanza, nel caso in cui oggetto della segnalazione sia una condotta delittuosa non ancora giunta a completo esaurimento o consumazione, i soggetti di cui all'art. 5 lett. a) e b) del Decreto debbono altresì attivarsi senza indugio al fine di impedire il compimento dell'azione o la realizzazione dell'evento (desistenza o recesso attivo di cui all'art. 56 c.p.), onde scongiurare il sorgere – in capo alla Società - della responsabilità amministrativa (a sensi dell'art. 26, comma secondo, D. Lgs. n. 231/2001).

II) Oltre alle segnalazioni relative alle violazioni, anche solo potenziali, sopra descritte, devono obbligatoriamente ed immediatamente essere trasmessi all'Organismo di Vigilanza alla casella di posta elettronica dedicata odv@allsystemgroup.it le seguenti informazioni, il più possibile circostanziate (l'elencazione che segue è puramente esemplificativa e non esaustiva), relative a:

- 1) modifiche sia organizzative sia relative alle procedure aziendali vigenti;
- 2) eventuali aggiornamenti del sistema dei poteri e delle deleghe;
- 3) procedure relative alla eventuale richiesta, erogazione ed utilizzo di contributi, finanziamenti, mutui agevolati o comunque altre erogazioni provenienti da parte dello Stato, Regioni, Comuni od altri enti pubblici o dalla Comunità europea;
- 4) reportistica periodica in materia di salute e di sicurezza sul lavoro nonché tutti i dati relativi agli infortuni sul lavoro occorsi;
- 5) il progetto di bilancio civilistico nonché il bilancio definitivamente approvato dall'Assemblea dei quotisti;
- 6) mancanze/violazioni sensibili ai fini del Decreto 231 commesse/ascrivibili/contestate nei confronti di soggetti terzi in rapporti con la Società ovvero provvedimenti assunti dalla Società nei confronti dei medesimi;
- 7) l'inizio del procedimento disciplinare nei confronti di personale della Società per illeciti involgenti violazioni del Modello 231 e del Codice Etico (eventualmente già oggetto di segnalazione riservata inviata mediante Procedura *Whistleblowing*): in particolare l'O.d.V. deve essere informato dell'apertura di un procedimento disciplinare, dell'incolpazione formulata nei confronti del soggetto sottoposto a procedimento disciplinare (ovvero dell'archiviazione del procedimento e della relativa motivazione) e degli esiti del medesimo;
- 8) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti per i quali è applicabile il D. Lgs. n. 231/2001, qualora tali indagini coinvolgano la Società o suoi Dipendenti od Organi Societari o comunque la responsabilità della Società stessa;
- 9) i provvedimenti e/o notizie provenienti da organi di polizia giudiziaria, o da qualsiasi altra autorità, fatti comunque salvi gli obblighi di segreto imposti dalla legge, dai quali si evinca lo svolgimento di indagini, anche nei confronti di ignoti, per gli illeciti in materia di tutela della sicurezza e della salute sul lavoro compreso l'avvio di procedimento giudiziario e/o amministrativo a carico di dipendenti/consulenti/apicali operanti nell'interesse della Società per le violazioni della normativa in materia di salute e sicurezza sul lavoro;
- 10) i rapporti predisposti dalle Direzioni aziendali, dai Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010, o dai Responsabili di filiale nell'ambito della loro attività di controllo, dai quali possano emergere fatti, atti, eventi od omissioni con profili di grave criticità rispetto all'osservanza delle norme del Decreto e dei protocolli di decisione;
- 11) i procedimenti disciplinari promossi o, nel caso in cui dette violazioni siano commesse da soggetti non dipendenti, le iniziative sanzionatorie assunte in via contrattuale nei loro riguardi.

III) Ciascuna Direzione aziendale o Responsabile di filiale a cui sia attribuito un determinato ruolo in una fase di un processo sensibile deve segnalare tempestivamente all'Organismo di Vigilanza eventuali propri comportamenti significativamente difformi da quelli descritti nel processo e le motivazioni che hanno reso necessario od opportuno tale scostamento. Ciascuna Direzione o Responsabile di filiale deve inviare un flusso ogni 3 mesi in cui dia atto di eventuali criticità rilevate rispetto alle prescrizioni contenute nel Codice Etico e nel Modello. Deve comunque inviare anche il flusso negativo attestando che non vi sono state criticità.

IV) Il Presidente del Consiglio di Amministrazione, in caso di eventi che potrebbero ingenerare gravi responsabilità di ALLSYSTEM ai sensi del D. Lgs. n. 231/2001, informa tempestivamente l'Organismo di Vigilanza e predisponde specifica relazione che descriva nel dettaglio l'evento stesso, il rischio, il personale coinvolto, le iniziative disciplinari in corso e le soluzioni per limitare il ripetersi dell'evento.

[La gestione delle segnalazioni rientranti nella Procedura *Whistleblowing* e delle comunicazioni/segnalazioni di natura diversa.](#)

Quanto alla gestione delle informazioni ricevute, l'O.d.V., valutate le segnalazioni, ove ritenuto utile/necessario, decide in ordine all'attività ispettiva eventualmente da compiere, utilizzando, all'uopo, le risorse interne o, se del caso, ricorrendo all'apporto di professionisti esterni, qualora l'attività ispettiva richieda specifiche e particolari competenze od in casi di particolare complessità.

Per le questioni connesse alla tutela della salute e sicurezza sul lavoro, l'O.d.V. potrà inoltre avvalersi delle risorse attivate dalla Società per la gestione dei relativi aspetti.

L'O.d.V., nell'ambito delle segnalazioni sensibili ai fini della Procedura *Whistleblowing*, deve agire garantendo che i soggetti segnalanti non siano oggetto di ritorsioni, discriminazioni o, comunque, penalizzazioni, dirette o indirette per motivi collegati, direttamente o indirettamente, alla segnalazione assicurando la riservatezza del soggetto che effettua la segnalazione (salvo la ricorrenza di eventuali obblighi di legge che impongano il disvelamento della relativa identità). Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare seguito adeguato alle stesse e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'art. 9 e del principio di cui agli articoli 5, paragrafo 1, lett. e), del Regolamento (UE) 2016/679 e 3, comma 1, lett. e), del D.Lgs. 51/2018. Non può, inoltre, essere rivelata, senza il consenso espresso del segnalante, a persone diverse da quelle competenti a ricevere o dare seguito alle segnalazioni, l'identità del segnalante (o qualsiasi altra informazione dalla quale la stessa possa evincersi).

Nell'ambito del procedimento disciplinare che dovesse sorgere in seguito a segnalazione di violazioni sensibili secondo la Procedura *Whistleblowing* ove la contestazione disciplinare

risulti fondata su accertamenti distinti e ulteriori rispetto alla sola segnalazione, non può essere rivelata l'identità del segnalante. Nel caso, invece, di contestazione fondata esclusivamente o anche solo parzialmente sulla segnalazione e la conoscenza dell'identità del segnalante risulti indispensabile per la difesa dell'incolpato, la segnalazione risulterà utilizzabile ai fini disciplinari nel solo caso di consenso espresso del segnalante alla rivelazione della propria identità.

La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della L. 7 agosto 1990, n. 241, nonché dagli articoli 5 e seguenti del D. Lgs. 14 marzo 2013, n. 33.

Nell'ambito della procedura di segnalazione la persona coinvolta può essere sentita, ovvero su richiesta della stessa, deve essere sentita anche mediante procedimento/interlocuzione cartolare.

Il *link* dedicato esclusivamente alla Procedura *Whistleblowing* idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante è <https://segnalazioni.allsystemgroup.com/#/>

Per tutte le comunicazioni/segnalazioni all'O.d.V. non rientranti nella Procedura *Whistleblowing* si rammenta l'indirizzo di posta elettronica 'ordinaria' (cd. 'peo') dell'Organismo di Vigilanza della ALLSYSTEM: **odv@allsystemgroup.it**

Flussi informativi periodici.

L'Organismo di Vigilanza esercita le proprie responsabilità di controllo anche mediante l'analisi di sistematici flussi informativi periodici trasmessi trimestralmente dalle Direzioni competenti di ALLSYSTEM, compresi gli Amministratori Delegati, il Datore di Lavoro ai sensi del D.Lgs. n. 81/2008, i Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010 e i Responsabili di filiale.

Con cadenza trimestrale i responsabili delle singole Direzioni aziendali coinvolte nei processi "sensibili" ai sensi del D. Lgs. n. 231/2001, i Direttori tecnici operativi ex D.M. n. 269 dell'1/12/2010 ed i Responsabili di filiale, mediante un processo di autovalutazione dell'attività svolta, certificano l'attuazione del Modello con particolare attenzione al rispetto dei principi di comportamento e delle norme operative previsti nel Codice Etico e nei Protocolli di decisione.

Attraverso questa formale attività di autovalutazione, evidenziano le eventuali criticità nei processi gestiti e gli eventuali disallineamenti rispetto alle indicazioni dettate dal Modello, dando contezza delle ragioni che hanno spinto la Direzione di appartenenza o la filiale a discostarsi dalle regole operative prescritte nel Modello.

B11) Designazione del Gestore del canale di segnalazione interno

ALLSYSTEM ha ritenuto conforme alle previsioni normative (art. 4, comma 2 D. Lgs. n. 24 del 2023) individuare Donatella Rista quale soggetto cui affidare la veste di Gestore del canale di segnalazione interno per le attività di ricezione, esame e valutazione delle segnalazioni, con

il compito [tra gli altri (sul punto si rinvia alla Procedura *Whistleblowing*, parte integrante del presente Modello di Organizzazione, Gestione e Controllo)] di:

- assicurare il corretto funzionamento delle procedure;
- condividere senza ritardo con l'O.d.V. della Società le segnalazioni di violazioni sensibili ai fini della disciplina recata nel Decreto 231/2001. Per violazioni 'sensibili' ai sensi della disciplina 231/2001 debbono intendersi le notizie di violazioni (consumate o tentate) consistenti nella realizzazione dei reati presupposto fonte di potenziale responsabilità amministrativa per l'Ente ovvero le infrazioni delle Procedure aziendali richiamate dal Modello di Organizzazione, Gestione e Controllo nonché del Modello stesso e del Codice Etico;
- coinvolgere l'O.d.V., laddove vi siano incertezze, nella valutazione della rilevanza ai sensi del Decreto 231/2001 della segnalazione ricevuta;
- inviare flussi informativi periodici mensili all'O.d.V. in merito alle segnalazioni ritenute dallo stesso Gestore non rilevanti ai sensi del Decreto 231/2001, al fine di consentire verifiche ad opera dello stesso O.d.V. sul corretto funzionamento del sistema e sulla qualità dello smistamento, anche in ottica di costante miglioramento del Modello;
- segnalare all'Organo amministrativo della Società le violazioni (non rilevanti ai fini 231/2001 ma) sensibili ai fini del D. Lgs. n. 24 del 2023. In particolare il Gestore del canale di segnalazione interna all'esito degli approfondimenti istruttori conseguenti alla ricezione e lavorazione della segnalazione, dovrà sottoporre al Soggetto titolare della potestà disciplinare i risultati dell'attività istruttoria.

Il Gestore del canale di segnalazione interna così designato è soggetto dotato delle necessarie competenze e formazione ed è tenuto a garantire imparzialità ed indipendenza nell'espletamento dell'incarico assegnatogli.

B12) Il sistema disciplinare.

Principi generali

L'efficacia del Modello è assicurata - oltre che dall'elaborazione di meccanismi di decisione e di controllo tali da eliminare o ridurre significativamente il rischio di commissione degli illeciti penali ed amministrativi per i quali è applicabile il D. Lgs. n. 231/2001 - dagli strumenti sanzionatori posti a presidio dell'osservanza delle condotte prescritte.

I comportamenti dei dipendenti e dei soggetti esterni (intendendosi per tali i lavoratori autonomi o parasubordinati, i professionisti, i consulenti, i fornitori, i componenti di ATI, i subappaltatori e tutti coloro che a vario titolo prestano collaborazione in favore di ALLSYSTEM) non conformi ai principi e alle regole di condotta prescritti nel presente Modello

- ivi ricomprendendo il Codice Etico e i protocolli operativi ad esso allegati - costituiscono illecito contrattuale.

Su tale presupposto, ALLSYSTEM adotterà nei confronti:

- del personale dipendente, le sanzioni disciplinari stabilite dalla contrattazione collettiva applicata dalla Società⁶;
- di tutti i soggetti esterni, il sistema sanzionatorio stabilito dalle disposizioni contrattuali e di legge che regolano la materia della risoluzione del contratto.

L'attivazione, sulla base delle segnalazioni pervenute dalle funzioni aziendali competenti o dall'Organismo di Vigilanza, lo svolgimento e la definizione del procedimento disciplinare nei confronti dei dipendenti sono affidati, nell'ambito delle competenze allo stesso attribuite come da atto costitutivo, all'Amministratore Delegato di ALLSYSTEM *pro tempore* che riveste la qualifica di Datore di lavoro o delegati.

Gli interventi sanzionatori nei confronti dei soggetti esterni sono affidati al Presidente del Consiglio di Amministrazione della società su segnalazione scritta del responsabile della direzione di impresa che gestisce il contratto o presso cui opera il lavoratore autonomo ovvero il fornitore.

Quanto precede verrà adottato indipendentemente dall'avvio e/o svolgimento e definizione dell'eventuale azione penale a carico dell'autore del fatto o della società, in quanto i principi e le regole di condotta imposte dal Modello sono assunte da ALLSYSTEM in piena autonomia ed indipendentemente dai possibili reati (o illeciti amministrativi) che eventuali condotte possano determinare e che l'autorità giudiziaria ha il compito di accertare.

L'art. 6, comma 2 *bis* del Decreto prevedeva, inoltre, nella formulazione ante novella del 2023, che nel sistema disciplinare così adottato venissero previste sanzioni specifiche nei confronti di chi avesse violato le misure di tutela del segnalante, nonché di chi avesse effettuato con dolo o colpa grave segnalazioni che si fossero rivelate infondate. Il testo novellato del comma 2 *bis* dell'art. 6 del Decreto non esplicita più tali prescrizioni le quali peraltro continuano ad essere coerenti e in linea con la nuova disciplina e, dunque, tuttora valido riferimento ai fini della implementazione del sistema disciplinare. Va altresì ricordato che, secondo quanto previsto dall'art. 21 comma secondo del D. Lgs. n. 24 del 2023 il Modello deve prevedere specifiche sanzioni nei confronti di coloro che si accerti, all'esito di giudizio disciplinare, essere responsabili delle condotte di cui alle lettere da a) a c) del primo comma del citato art. 21.

⁶ In particolare, il sistema disciplinare per il personale dipendente applicato da ALLSYSTEM è quello stabilito dal Contratto Collettivo Nazionale di Lavoro 1° febbraio 2013, così come rinnovato il 31 maggio 2023, per i dipendenti da Istituti e Imprese di Vigilanza privata e servizi fiduciari.

La verifica dell'adeguatezza del sistema sanzionatorio, il costante monitoraggio dei procedimenti di irrogazione delle sanzioni nei confronti dei dipendenti, nonché degli interventi nei confronti dei soggetti esterni sono affidati all'Organismo di Vigilanza, il quale procede anche alla segnalazione delle infrazioni di cui viene a conoscenza nello svolgimento delle funzioni che gli sono proprie e chiede conto dell'irrogazione o della mancata irrogazione delle sanzioni disciplinari a fronte delle contestazioni elevate.

Pertanto, in applicazione dei suddetti criteri, viene stabilito il sistema sanzionatorio di seguito disciplinato.

B12 – I) Personale dipendente (art. 101 e seguenti CCNL).

Le violazioni delle regole comportamentali previste dal Modello commesse dai lavoratori dipendenti costituiscono inadempimento contrattuale e pertanto potranno comportare l'adozione delle sanzioni disciplinari previste e disciplinate dal contratto collettivo applicabile al medesimo rapporto di lavoro, ferme restando la diversa natura e la conseguente autonomia del potere disciplinare in capo al Questore ex art. 6 del r.d. 1952/1935 convertito in legge 508/1936.

In particolare, il C.C.N.L. per i dipendenti da aziende esercenti attività del settore della vigilanza privata e dei servizi fiduciari del 1° febbraio 2013 e rinnovato il 31 maggio 2023, stabilisce agli artt. 101 e seguenti l'applicazione delle seguenti sanzioni disciplinari a fronte di inadempimenti contrattuali di crescente gravità:

- a) rimprovero verbale o scritto;
- b) multa non eccedente l'importo di quattro ore della retribuzione giornaliera;
- c) sospensione dalla retribuzione e dal servizio per un periodo da 1 a 6 giorni;
- d) licenziamento per giusta causa.

Restano ferme, e si intendono qui richiamate, le disposizioni dello Statuto dei Lavoratori (art. 7 e seguenti Legge 20 maggio 1970, n. 300, richiamata dallo stesso C.C.N.L. sub art. 104) in merito alla procedura applicativa delle sanzioni disciplinari e all'obbligo di esposizione del codice disciplinare all'interno dell'impresa.

In conformità ai criteri ispiratori *in subiecta materia* previsti anche dallo Statuto dei Lavoratori, la tipologia e l'entità della sanzione (laddove sia previsto un minimo e un massimo edittale) saranno individuate tenendo conto della gravità della mancanza, della recidiva nella medesima, del grado della colpa e dell'intensità della volontarietà che hanno caratterizzato la condotta sussumibile in un illecito disciplinare.

Quali criteri ulteriori per commisurare la sanzione all'illecito commesso, si individuano le seguenti circostanze, a titolo meramente esemplificativo:

- **criteri obiettivi:**

- 1) il livello di responsabilità connesso alle mansioni esercitate dal dipendente;
- 2) l'eventuale commissione del fatto con la cooperazione colposa o il concorso deliberato di altri dipendenti;
- 3) eventuali precedenti specifici e non nell'arco del biennio;
- 4) la rilevanza, ai fini dell'osservanza del Decreto legislativo n. 231/2001, degli obblighi violati;
- 5) l'entità del danno, anche di mera immagine, derivante alla ALLSYSTEM, dalla commissione dell'illecito in contestazione.

- **criteri soggettivi:**

l'elemento soggettivo – colpa lieve o grave, dolo generico, intenzionale, eventuale o di impeto – che ha animato la condotta del dipendente.

Dovendo correlare le sanzioni disciplinari previste dal C.C.N.L. alle condotte violative degli obblighi discendenti dall'osservanza del Decreto n. 231/2001, dal Codice Etico e dal presente Modello (Parte Generale, Parte Speciale, Procedura *Whistleblowing*) nonché dai protocolli operativi dal medesimo richiamati, si individuano qui di seguito i criteri applicativi:

1) il provvedimento del **rimprovero scritto** si applica in caso di:

lieve inosservanza dei principi e delle regole di comportamento previsti dal presente Modello ovvero adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello, qualora le medesime condotte siano state animate da mera negligenza operativa, correlandosi detto comportamento ad una condotta di minor gravità del lavoratore *“per lievi irregolarità nell'adempimento dei suoi doveri o nel comportamento di servizio”*, ai sensi di quanto previsto dall'art. 101, lett. a) del Codice disciplinare vigente.

A titolo esemplificativo, tra tali comportamenti rientra la ritardata segnalazione all'Organismo di Vigilanza delle informazioni da trasmettere nei periodici flussi ai sensi del presente Modello; l'archiviazione disordinata o scorretta di documentazione comprovante l'osservanza delle prescrizioni del presente Modello; la mancata partecipazione anche ad una sola sessione di formazione proprio in materia di responsabilità amministrativa. Con riferimento alla inosservanza delle disposizioni previste dal Decreto legislativo n. 81/2008 e da tutta la normativa in materia di sicurezza sul lavoro applicabile in relazione alle attività svolte, si considera meritoria della sanzione in esame qualsiasi anche lievissima inosservanza delle disposizioni citate.

2) Il provvedimento della **multa in misura non eccedente le 4 ore della retribuzione giornaliera** si applica in caso:

di inosservanza non lieve dei principi e delle regole di comportamento previste dal presente Modello ovvero adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello o del Codice Etico in misura tale da poter essere considerata ancorché non lieve, comunque, non grave, e animata da una negligenza o imperizia più gravi di quelle di cui al capo 1); correlandosi detto comportamento ad una condotta del dipendente che *“esegua senza la necessaria diligenza il lavoro affidatogli”* ai sensi di quanto già previsto dall'art. 101, lett. B) del Codice disciplinare vigente, anche con riferimento a condotte di maggior gravità rispetto a quelle sanzionabili con il mero rimprovero scritto o in caso di recidiva nelle violazioni di cui al punto 1).

A titolo esemplificativo, tra tali comportamenti rientra la mancata segnalazione all'Organismo di Vigilanza delle informazioni da trasmettergli periodicamente; la reiterata mancata partecipazione, senza giustificato motivo, alle sessioni formative che nel tempo verranno predisposte dalla ALLSYSTEM per sensibilizzare i dipendenti all'osservanza del Decreto n. 231/2001 e al presente Modello; l'omissione della dovuta vigilanza sul comportamento del personale operante all'interno della sfera di responsabilità del responsabile della direzione o della filiale. Con riferimento alla inosservanza delle disposizioni previste dal Decreto n. 81/2008 e da tutta la normativa in materia di sicurezza sul lavoro applicabile in relazione alle attività svolte, si considera meritoria della sanzione in esame qualsiasi inosservanza delle disposizioni citate da cui sia derivato un evento lesivo rientrante nel concetto di lesione colposa lieve o qualsiasi inosservanza da parte delle guardie giurate o degli operatori fiduciari in materia di tempestiva doverosa segnalazione di anomalie di funzionamento dei mezzi di trasporto, di inadeguata conservazione o porto dei DPI, di condotta di guida pericolosa e tale da mettere a repentaglio la sicurezza delle altre guardie particolari giurate o degli altri operatori fiduciari che utilizzino gli stessi mezzi.

3) Il provvedimento della **sospensione dalla retribuzione e dal servizio da 1 a 6 giorni** si applica in caso:

di inosservanza grave dei principi e delle regole di comportamento previste dal presente Modello ovvero adozione, nell'ambito delle aree sensibili, di un comportamento non conforme o non adeguato alle prescrizioni del Modello o del Codice Etico in misura tale da essere considerata di una certa gravità; correlandosi detto comportamento ad una condotta del dipendente che *“esegua con negligenza grave il lavoro affidatogli”* o *“ometta parzialmente di eseguire il servizio assegnato”* o *“non avverta subito i superiori di eventuali irregolarità nell'adempimento del servizio”* ai sensi di quanto già previsto dall'art. 101 lett. C) del Codice disciplinare vigente, anche con riferimento a condotte di maggior gravità rispetto a quelle sanzionabili con la multa non superiore all'importo di quattro ore di retribuzione o in caso di recidiva nelle violazioni di cui al punto 2).

A titolo esemplificativo, tra tali comportamenti rientra l'inosservanza delle prescrizioni del Codice Etico, l'inosservanza delle disposizioni dei poteri di firma e del sistema delle deleghe vigente in ALLSYSTEM; la reiterata mancata partecipazione, senza giustificato motivo, alle

sessioni formative che nel tempo verranno predisposte dalla ALLSYSTEM per sensibilizzare i dipendenti all'osservanza del Decreto n. 231/2001 e al presente Modello; l'omessa segnalazione ad ALLSYSTEM quale datore di lavoro facoltizzato all'esercizio del potere disciplinare di comportamenti integranti illecito disciplinare da parte del personale sottoposto alla propria vigilanza nell'area della ortodossia dei rapporti con la Pubblica Amministrazione, sia essa cliente, sia essa ente che rilascia i titoli abilitativi all'esercizio dell'attività aziendale, che su di essa vigili (Questura e Prefettura), sia essa ente ispettivo; qualsiasi violazione da parte degli stessi e di tutti gli altri dipendenti delle prescrizioni in materia di sicurezza sul lavoro da cui sia derivata una lesione colposa grave o che integri una seconda violazione in quelle stabilite al punto 2), con particolare riferimento anche alla tematica della corretta detenzione e porto dei DPI; l'erronea segnalazione *whistleblowing* nel caso di cui all'art. 16, comma 3 D. Lgs. n. 24/2023 in presenza di accertata colpa grave del segnalante; l'omesso svolgimento delle attività di verifica e analisi delle segnalazioni riservate *whistleblowing* ricevute dal Gestore del canale di segnalazione a tal fine designato dalla Società; l'adozione di condotte volte ad impedire/ritardare l'attività di verifica e analisi delle segnalazioni *whistleblowing* ovvero la colposa violazione dell'obbligo di riservatezza posto a tutela del segnalante (o dei soggetti ad esso equiparati ai fini di tutela dal D. Lgs. n. 24 del 2023); la inveritiera segnalazione *whistleblowing* nel caso di cui all'art. 16, comma terzo, D. Lgs. n. 24 del 2023 in presenza di accertata colpa grave del segnalante.

4) Il provvedimento del **licenziamento per giusta causa** si applica in caso:

di adozione, nell'espletamento delle attività ricomprese nelle aree sensibili per la realtà di impresa di ALLSYSTEM, di un **comportamento caratterizzato da notevole reiterato grave inadempimento o deliberato contrasto** delle prescrizioni e/o delle procedure e/o delle norme interne stabilite dal presente Modello o del Codice Etico anche con accettazione del rischio del verificarsi di situazioni prodromiche alla commissione di un illecito presupposto, correlandosi detto comportamento alla condotta del lavoratore che *"commetta una mancanza che non consenta la prosecuzione, anche provvisoria, del rapporto di lavoro"* come previsto all'art. 101, lettera D), del Codice disciplinare vigente.

A titolo esemplificativo, tra tali comportamenti rientrano le condotte intenzionali di reiterata inosservanza delle prescrizioni del presente Modello; omessa comunicazione all'Organismo di Vigilanza di comunicazioni rilevanti quali la notificazione di informazioni di garanzia per delitti rientranti tra i reati presupposto ai sensi del Decreto n. 231/2001 o verbali amministrativi per violazioni gravi di disposizioni legislative e/o amministrative a presidio della sicurezza sul lavoro ai sensi del Decreto n. 81/2008; il comportamento consapevolmente diretto alla commissione di un reato presupposto ai sensi del Decreto 231/2001, la condotta di falsificazione anche per omissione dei report destinati all'ODV nelle aree sensibili per l'attività di ALLSYSTEM, l'ostacolo anche surrettizio ai controlli, l'impedito accesso alle informazioni o alla documentazione da parte dei soggetti preposti ai controlli o alle decisioni in aree sensibili; la propaganda di idee fondate sulla superiorità o sull'odio

razziale o etnico ovvero la commissione, anche sotto forma di istigazione, a commettere atti di discriminazione nonché atti di violenza o di provocazione alla violenza per motivi razziali, etnici, nazionali o religiosi; relativamente all'area della sicurezza sul lavoro, qualsiasi violazione delle prescrizioni in materia di sicurezza sul lavoro da cui siano derivati una lesione colposa gravissima o l'omicidio colposo; la consapevole violazione dell'obbligo di riservatezza posto a tutela del segnalante (o dei soggetti ad esso equiparati ai fini di tutela dal D. Lgs. n. 24/2023) ovvero l'intenzionale realizzazione di condotte ritorsive a seguito (e per il fatto) di segnalazione *whistleblowing* (riservata o, *ab origine*, anonima che sia) o, ancora, la dolosa realizzazione di condotte (attive od omissive) di ostacolo alla segnalazione *whistleblowing* o, infine, la non veritiera segnalazione *whistleblowing* nel caso di cui all'art. 16, comma terzo, D. Lgs. n. 24 del 2023 in presenza di accertato dolo del segnalante.

A tali comportamenti si equiparano l'omessa reiterata segnalazione all'Amministratore Delegato di ALLSYSTEM, quale datore di lavoro facoltizzato all'esercizio del potere disciplinare di comportamenti integranti illecito disciplinare da parte del personale sottoposto alla propria vigilanza, di qualsiasi violazione delle prescrizioni in materia di sicurezza sul lavoro da cui sia derivata una lesione colposa gravissima o che rappresenti la reiterazione delle violazioni di cui al punto 3).

B12 – II) Dirigenti.

In caso di violazione, da parte dei dirigenti, dei principi, delle regole e delle procedure interne previste nel presente Modello o di adozione, nell'espletamento di attività ricomprese nelle aree sensibili, di un comportamento non conforme alle prescrizioni del Modello stesso, si provvederà ad adottare i provvedimenti di seguito indicati, tenuto conto della gravità della violazione e della sua eventuale reiterazione. In considerazione del particolare vincolo fiduciario che caratterizza il rapporto tra ALLSYSTEM e i dirigenti, in conformità alle disposizioni di legge vigenti, si procederà con il licenziamento con preavviso o senza preavviso in caso di violazione grave e intenzionale delle prescrizioni contenute nel Modello o di recidiva nelle violazioni connotate da colpa grave.

Nel caso delle infrazioni meno gravi, la società si riserva la facoltà di applicare la misura del rimprovero scritto in caso di inosservanza dei principi e delle regole di comportamento previste dal Modello connotata da colpa lieve.

B12 – III) Componenti del Consiglio di Amministrazione.

In caso di violazione del Modello, delle Procedure e/o delle norme interne previste e/o richiamate nei protocolli operativi allegati al Modello, nonché del Codice Etico da parte di soggetti che ricoprono la funzione di componenti del Consiglio di Amministrazione della Società, l'Organismo di Vigilanza informerà l'Assemblea dei Soci la quale provvederà ad adottare le iniziative ritenute opportune (convocazione Assemblea dei Soci con esclusione del socio che sia anche Consigliere di Amministrazione cui sia addebitabile la violazione accertata) in relazione alla fattispecie, nel rispetto della normativa civilistica.

B12 – IV) Componenti del Collegio Sindacale.

In caso di violazione del Modello, delle Procedure e/o delle norme interne previste e/o richiamate nei protocolli operativi allegati al Modello, nonché del Codice Etico da parte di componenti del Collegio Sindacale, l'Organismo di Vigilanza informerà il Consiglio di Amministrazione, il quale provvederà ad assumere tutte le opportune iniziative da adottarsi con le procedure previste dalla normativa civilistica (tra le quali ad esempio, la convocazione dell'Assemblea dei soci, allo scopo di mettere in atto i provvedimenti del caso).

B12 – V) Soggetti esterni.

Ogni comportamento posto in essere da soggetti esterni ad ALLSYSTEM che, in contrasto con il presente Modello, sia suscettibile di comportare il rischio di commissione di uno degli illeciti per i quali è applicabile il Decreto n. 231/2001, determinerà, secondo quanto previsto dalle specifiche clausole contrattuali inserite nelle lettere di incarico, nei contratti di fornitura, negli accordi che presiedono alla costituzione di ATI, nei contratti di subappalto, nei contratti di consulenza e in qualsiasi altra convenzione scritta con fornitori della Società, *partner* in associazioni temporanee, consorzi e qualsivoglia altra forma di associazione con società del settore, la risoluzione anticipata del rapporto contrattuale, fatta ovviamente salva l'ulteriore riserva di richieste di risarcimento dei danni qualora da tali comportamenti derivi qualsivoglia danno (anche di sola immagine o reputazione) ad ALLSYSTEM, come nel caso di applicazione da parte dell'Autorità Giudiziaria delle sanzioni previste dal Decreto medesimo.

Medesime clausole contrattuali verranno inserite nei contratti già in essere previa comunicazione ai soggetti esterni dell'intervenuta adozione del presente Modello da parte del Presidente del Consiglio di Amministrazione.

B13) La diffusione del Modello.

L'adeguata diffusione dei principi e delle prescrizioni contenute nel Modello rappresenta fattore di grande importanza per la corretta ed efficace attuazione del sistema di prevenzione aziendale. A tale proposito la Società ha definito un piano di comunicazione e formazione finalizzato a diffondere ed illustrare a tutto il personale il Modello.

Il piano è gestito dalla funzione Legale e dalla funzione Qualità in collaborazione con l'Organismo di Vigilanza.

B13 – I) Il piano di comunicazione.

L'adozione del presente Modello è comunicata ai Destinatari attraverso l'invio di una lettera a firma del Presidente del Consiglio di Amministrazione.

Il Modello verrà consegnato a tutti i dipendenti. Al momento del ritiro i dipendenti dovranno firmare una dichiarazione di ricevuta.

Ai nuovi assunti sarà data comunicazione dell'adozione del Modello, nonché fornita copia elettronica o cartacea dello stesso e del Codice Etico, unitamente alla documentazione prevista in sede di assunzione.

Tutte le successive modifiche e informazioni concernenti il Modello saranno tempestivamente comunicate ai Destinatari attraverso i canali informativi ufficiali.

B13 – II) Il piano di formazione.

La formazione del personale ai fini dell'attuazione del Modello è gestita dalla funzione Legale e dalla funzione Qualità in collaborazione con l'Organismo di Vigilanza.

Si prevedono interventi diversificati a seconda del target, in un'ottica di personalizzazione dei percorsi e di reale rispondenza ai bisogni delle singole Direzioni/risorse. Pertanto, in linea generale, la Società prevede l'erogazione di corsi che illustrino, secondo un approccio modulare:

- il contesto normativo e giurisprudenziale;
- il Modello organizzativo adottato dalla Società e i relativi Allegati;
- la gestione del Modello nel continuo e il ruolo dell'Organismo di Vigilanza.

La partecipazione ai momenti formativi sarà formalizzata attraverso la richiesta della firma di presenza e l'inserimento nella banca dati dell'Organismo di Vigilanza dei nominativi dei presenti, nonché attraverso la somministrazione di test obbligatori.

La Funzione Legale, in cooperazione con l'Organismo di Vigilanza, cura che il programma di formazione sia adeguato ed efficacemente attuato.

B14) L'aggiornamento del Modello.

L'efficacia e la concretezza del Modello vengono valutate anche con riferimento alla dinamicità dello stesso, ovvero alla capacità di seguire i cambiamenti organizzativi della Società e del contesto normativo di riferimento. Ciò determina la necessità di procedere, da parte dell'Organismo di Vigilanza, ad una costante attività di aggiornamento del Modello.

ALLSYSTEM attribuisce al Consiglio di Amministrazione il potere di adottare, sulla base anche di indicazioni e proposte provenienti dall'Organismo di Vigilanza, modifiche e/o integrazioni al Modello ed ai suoi Allegati che si dovessero rendere necessarie in conseguenza di:

- significative violazioni delle prescrizioni del Modello adottato;
- modifiche normative che comportino l'estensione della responsabilità amministrativa degli enti ad altre tipologie di reato per le quali si reputi sussistente un rischio di commissione nell'interesse o a vantaggio della Società;

- significative modifiche intervenute nella struttura organizzativa, nel sistema dei poteri e nelle modalità operative di svolgimento delle attività a rischio e dei controlli a presidio delle stesse.

ALLEGATI

- 1) ELENCO DEI REATI E DEGLI ILLECITI AMMINISTRATIVI RILEVANTI AI SENSI DEL DECRETO N. 231/2001 E GRADO DI RISCHIO DI COMMISSIONE DEGLI ILLECITI PRESUPPOSTO**
- 2) CODICE ETICO DI ALLSYSTEM S.P.A.**
- 3) PROCEDURA “WHISTLEBLOWING”**
- 4) PROTOCOLLI DI DECISIONE NELLE AREE RITENUTE PIU’ SENSIBILI**

ALLEGATO 1 - ELENCO DEI REATI E DEGLI ILLECITI AMMINISTRATIVI RILEVANTI AI SENSI DEL DECRETO N. 231/2001 E GRADO DI RISCHIO DI COMMISSIONE DEGLI ILLECITI PRESUPPOSTO

REATO	ARTICOLO	FATTISPECIE	MODALITA' DI REALIZZAZIONE	SOGGETTI O AREA COINVOLTA	GRADO DI RISCHIO	
A) REATI DI OMICIDIO COLPOSO E LESIONI COLPOSE GRAVI O GRAVISSIME, COMMESSI CON VIOLAZIONE DELLE NORME SULLA TUTELA DELLA SALUTE E SICUREZZA SUL LAVORO Art. 25-septies D.Lgs 231/01						
1. Omicidio colposo	Art. 589 C.P.	L'omicidio colposo e le lesioni personali colpose sono fattispecie astrattamente a rischio di commissione in AllSystem S.p.A. in quanto la tipologia di attività svolta presenta soglie di rischio elevate per la sicurezza del personale e per la salute del personale	Tale reato può configurare un vantaggio di AllSystem S.p.A. rappresentato dai risparmi di spesa derivanti, per esempio, dalla mancata adozione delle necessarie misure antinfortunistiche e dei dispositivi di protezione, dalla non effettuazione "a regola" delle manutenzioni su automezzi, dalla non completa e corretta formazione del personale in relazione all'utilizzo dei sistemi di safety (giubbotti antiproiettile, cinture di sicurezza, ecc.) o sulle misure di sicurezza, da mancati controlli sull'effettivo apprendimento da parte del personale (Guardie giurate ed autisti in primis) delle prescrizioni sulle regole di sicurezza, ecc.	Amministratori della società	8	alto
				Datore di lavoro		
				RSP		
				ASPP		
				Responsabili di filiale o degli automezzi		
2. Lesioni personali colpose	Art. 590 co.3 C.P.			Il reato si può anche ascrivere a titolo di cooperazione colposa fra tutti o alcuni di questi soggetti	8	alto
B) RICETTAZIONE, RICICLAGGIO E IMPIEGO DI DENARO, BENI O UTILITA' DI PROVENIENZA ILLECITA NONCHE' AUTORICICLAGGIO Art. 25-octies D.Lgs. 231/01						
1. Ricettazione	Art. 648 C.P.	Le ipotesi di reato sopra indicate sono concretamente applicabili ad AllSystem S.p.A.				
2. Riciclaggio	Art. 648-bis C.P.					
3. Impiego di denaro, beni o utilità di provenienza illecita	Art. 648-ter C.P.					
4. Autoriciclaggio	Art. 648-ter1 C.P.					
C) REATI DI FALSITA' IN MONETE, CARTE DI PUBBLICO CREDITO, VALORI DI BOLLO E IN STRUMENTI O SEGNI DI RICONOSCIMENTO Art. 25-bis D. Lgs. 231/01						

1. Falsificazione di monete, spendita ed introduzione nello Stato, previo concerto, di monete falsificate	Art. 453 C.P.				
2. Alterazione di monete	Art. 454 C.P.				
3. Spendita e introduzione nello Stato, senza concerto, di monete falsificate	Art. 455 C.P.				
4. Spendita di monete falsificate ricevute in buona fede	Art. 457 C.P.	Le ipotesi di reato in esame non si ritengono realizzabili in AllSystem S.p.a. in quanto nel luglio 2020 la società ha ceduto il ramo d'azienda inerente il trasporto e la conta valori			
5. Falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione dei valori di bollo falsificati	Art. 459 C.P.			0	nullo
6. Contraffazione di carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo	Art. 460 C.P.				
7. Fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigrana	Art. 461 C.P.				
8. Uso di valori di bollo contraffatti o alterati	Art. 464 C.P.				
9. Contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni	Art. 473 C.P.				
10. Introduzione nello Stato e commercio di prodotti con segni falsi	Art. 474 C.P.				

D) REATI SOCIETARI Art. 25-ter D.Lgs. 231/01

1. Indebita restituzione di conferimenti	Art. 2626 C.C.	Sono fattispecie che non rappresentano concretamente allo stato attuale un rischio per AllSystem S.p.A. in quanto non sono stati restituiti conferimenti o vi è stata ripartizione di utili o riserve illegale, il capitale sociale è formato ad oggi da conferimenti in denaro interamente versati, né è in atto una procedura di liquidazione. In ogni caso, non si esclude che in futuro potrebbero verificarsi condizioni tali da configurare le ipotesi di reato (es. in caso di cambiamenti nella compagine societaria, liquidazione, ecc.) per cui almeno a livello di Linee Guida o Codice Etico appare opportuno prescrivere modalità di comportamento adeguate.				
2. Illegale ripartizione degli utili e delle riserve	Art. 2627 C.C.					
3. Illecite operazioni sulle azioni o quote sociali o della società controllante	Art. 2628 C.C.					
4. Formazione fittizia del capitale	Art. 2632 C.C.			0	nullo	
5. Indebita ripartizione dei beni sociali da parte dei liquidatori	Art. 2633 C.C.					
6. False comunicazioni sociali della società quotata	Art. 2622 bis c.c	Non paiono oggi applicabili ad AllSystem S.p.A. per la sua natura (società non			0	nullo

7. Omessa comunicazione del conflitto di interessi	Art. 2629 bis c.c.	quotata), per la sua attività (non tratta strumenti finanziari rivolti al pubblico) e la sua rilevanza (non è società che ragionevolmente possa trattare informazioni price sensitive).				
8. Aggiotaggio	Art. 2637 c.c.					
8. False comunicazioni sociali	Art. 2621 e 2622 c.c.	<p>Il reato si realizza con l'esposizione o nell'omissione nei bilanci, di voci e poste atte a rappresentare la reale situazione economico-patrimoniale e finanziaria dell'Azienda. Tale reato può configurarsi in AllSystem S.p.A. qualora il Consiglio di Amministrazione o uno degli Amministratori intervenissero in poste di rettifica o valutazione di bilancio, al fine di manipolare la percezione della reale situazione economico-finanziaria dell'Azienda.</p>	<p>- Accantonamento al fondo svalutazione crediti / perdite su crediti: l'ipotesi di reato potrebbe configurarsi come mancata effettuazione di proposito di <u>svalutazione di alcuni crediti</u> di importo rilevante, per non contabilizzare in bilancio una componente negativa di reddito.</p> <p>- Determinazione delle fatture da emettere e/o dei lavori in corso effettuati su commessa. La fatturazione attiva avviene solitamente a canone temporale, a intervento o nel caso di avanzamento lavori su commessa, a SAL. La quantificazione del SAL può rappresentare un'area di ipotetico rischio qualora i soggetti atti a valorizzare questa posta, effettuassero valutazioni non rispondenti al vero per importi significativi atti ad alterare il bilancio.</p> <p>- Non rilevazione in bilancio di voci di <u>accantonamenti per rischi</u> concreti e significativi es. rischi legali o per cause con il personale.</p>	<p>- Direzione Aziendale in prima istanza;</p> <p>- Amministrazione in ordine all'attività operativa di supporto alla Direzione;</p> <p>- Aree aziendali coinvolte nella rendicontazione, sempre in supporto dell'Amministrazione.</p>	4	medio
9. Impedito controllo	Art. 2625 c.c.	La fattispecie potrebbe configurarsi qualora gli amministratori ponessero in essere artifici volti a non consentire alla compagine sociale o al Collegio sindacale o alla società di revisione di effettuare i controlli previsti dalla legge	La fattispecie è oggi ipotizzabile in quanto AllSystem S.p.A. ha una compagine sociale composta, alcuni Organi di controllo quali il Collegio Sindacale e la società di revisione che certifica i bilanci ed Organi decisionali quali Comitato Esecutivo e Consiglio di Amministrazione.	<p>- Direzione Aziendale/Amministratore;</p> <p>- Amministrazione;</p> <p>- Altre aree che eventualmente prendessero parte al processo di verifica di cui sopra.</p>	1	basso

10. Corruzione tra privati	Art. 2635, 3° comma, e 2635 bis, 1° comma c.c.	La fattispecie potrebbe configurarsi in AllSystem S.p.A. prevalentemente nei casi di stipula ed esecuzione di contratti attivi con soggetti terzi privati o trattative con i Sindacati nel caso di cause di lavoro o trattative sindacali, a vantaggio di AllSystem S.p.A. ed a nocumento di una corretta attività sindacale.	<p>- Stipula ed esecuzione di contratti con terzi privati: l'Azienda dal punto di vista commerciale e produttivo si trova a trattare con i clienti terzi privati. I rapporti commerciali sono tracciati sul CRM (Customer Relationship Management), sistema di gestione "commerciale" del cliente, mentre l'avanzamento delle attività tecniche è – ai fini di controllo interno – periodicamente analizzato dalla Direzione, dai Commerciali, e dai Responsabili di Commessa.</p> <p>- Trattative sindacali: le filiali o l'area Legale si interfacciano con le associazioni sindacali sia per motivazioni legate alla contrattualistica (rinnovo del contratto, applicazione di normativa. Ecc.) sia nel caso di contestazioni – provvedimenti disciplinari – cause, ecc.</p>	<p>- Direzione Aziendale</p> <p>- Area Commerciale: i commerciali sono infatti il trait d'union tra le Aziende</p> <p>- Responsabili di filiale qualora i contratti attivi venissero stipulati direttamente mediante il loro intervento o qualora gestissero direttamente i rapporti con i sindacati</p> <p>- Ufficio Gare qualora si trattasse di clientela acquisibile tramite gara</p> <p>- Ufficio Personale, Privacy e Recruitment qualora la corruzione si realizzasse mediante assunzione di parenti o persone collegate a personale del partner commerciale o nei rapporti con i sindacati</p> <p>- Area Legale prevalentemente nell'ambito dei rapporti con i sindacati</p> <p>- Amministrazione qualora la corruzione si realizzasse mediante pagamenti "fittizi" o fraudolenti o non rilevasse flussi finanziari anomali facilmente individuabili.</p>	8	alto
11. Illecita influenza sull'assemblea	Art. 2636 c.c.	La fattispecie potrebbe configurarsi qualora alcuni degli amministratori ponessero in essere fraudolentemente artifizii volti a influenzare, per un supposto vantaggio di AllSystem S.p.A.,	La fattispecie è oggi ipotizzabile anche se remoto, in quanto la maggioranza assoluta delle azioni di AllSystem S.p.A., pur avendo una compagine sociale composita, è detenuta dal sig. Serrani che è anche Presidente del Consiglio di Amministrazione che è coinvolto operativamente nella	<p>- Direzione Aziendale/Amministratore</p> <p>- Amministrazione.</p>	1	basso

		la compagine sociale della società e la maggioranza dell'assemblea.	gestione aziendale.			
12. Ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (con riguardo a tale ipotesi di reato, la cessione del ramo d'azienda inerente il trasporto e la conta valori intervenuto nel luglio 2020 ha reso parzialmente non attuali le valutazioni che seguono, che tuttavia restano parte integrante del modello nel caso in cui la AllSystem decidesse di espandere nuovamente la propria attività)	Art. 2638 c.c.	La fattispecie di reato potrebbe configurarsi in AllSystem S.p.A., prevalentemente nell'attività di conta e custodia di denaro e nel caso di ispezioni	- Attività di conta e custodia di denaro: per detta attività All System è frequentemente soggetta a controlli ed ispezioni di Banca d'Italia presso le sale conta. Con artifizii o raggiri, o comunicando periodicamente giacenze difformi dal vero, impedire il corretto svolgimento dei controlli di Bankitalia.	- Direzione Aziendale/Amministratori;	4	medio
			-Nel caso di ispezioni ad es. a livello Europeo, del rispetto delle norme di sicurezza di alcuni particolari "cantieri" quali Aeroporto "Sandro Pertini" di Caselle (TO), Expo 2015 o similari.	- Nel caso di controlli su cantieri: Datore di Lavoro, RSPP, Direttore Tecnico, Security Manager, altri soggetti relativi al cantiere; - Nel caso di attività di sala conta: Datore di Lavoro, Responsabili Sala conta, Security Manager.		
13. Delitto di false o omesse dichiarazioni per il rilascio del certificato preliminare previsto dalla normativa attuativa della direttiva (UE) 2019/2121	Art. 54 D.Lgs. 19/2023	Non si ritiene ragionevolmente applicabile in AllSystem S.p.A.			0	nullo
E) REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE Art. 25 D.Lgs. 231/01						
1. Induzione indebita a dare o promettere utilità 2. Corruzione per l'esercizio della funzione	Art. 319 quater C.P. Art. 318 C.P.	Le fattispecie di reato possono configurarsi in capo ad AllSystem S.p.A. ogni qualvolta un soggetto dipendente o apicale, venga in contatto con Pubblici ufficiali o Incaricati di Pubblico Servizio, sia per attività ordinarie, periodiche ispezioni da parte di Enti Pubblici (quali ad esempio la Banca D'Italia), sia nel caso di atti giudiziari (contenziosi).	- Partecipazione a bandi e ad appalti pubblici: il rischio è stato ridotto rispetto al passato in quanto la società ha mostrato attenzione al rispetto delle indicazioni contenute nel Protocollo n. 5 di Parte Speciale del MOG. Tuttavia la Società non ha rinnovato dopo il 2021 la certificazione ISO 37001:2016 (prevenzione della corruzione)	- Direzione Aziendale; - Area Commerciale con particolare riferimento all'Ufficio Gare; - Area Amministrazione; - Area personale, Privacy, Recruitment	6	medio
			- Gestione pratiche di accertamento: il rischio risulta essersi attenuato di poco rispetto al passato	- Direzione Aziendale; - Area Risorse Umane;		
3. Corruzione per atto contrario ai doveri di ufficio	Art. 319 C.P.				4	medio

			stante l'adozione del Protocollo n. 7 di Parte Speciale del MOG e la riferita maggiore attenzione rispetto al passato nel corso delle visite ispettive	- Area Amministrazione.		
4. Corruzione in atti giudiziari	Art. 319-ter C.P.		- Partecipazione a processi o ad atti giudiziari: il rischio risulta essersi attenuato di poco rispetto al passato stante l'adozione del Protocollo n. 8 di Parte Speciale del MOG e la registrata maggiore attenzione rispetto al passato	- Direzione Aziendale;	4	medio
5. Corruzione di persona incaricata di un pubblico servizio	art. 320 c.p.			- Area Legale;		
6. Pene per il corruttore	Art. 321 C.P.			- Area Amministrazione;		
7. Traffico di influenze illecite	Art. 346-bis C.P.			- Area personale.		
8. Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri della Corte penale internazionale o degli organi delle Comunità europee e di funzionari delle Comunità europee e di Stati esteri	Art. 322-bis C.P.	Non si ritengono fattispecie applicabili ad AllSystem S.p.A. in quanto l'azienda non ha ruoli di Pubblico ufficiale o incaricato di Pubblico Servizio né ha contatti abituali con organi o funzionari della Comunità Europea o Stati Esteri.			0	nullo
9. Peculato, peculato mediante profitto dell'errore altrui, abuso d'ufficio (limitatamente alle condotte che ledono gli interessi finanziari dell'Unione Europea)	Artt. 314, co. 1, 316 e 323 C.P.	Non si ritengono fattispecie applicabili ad AllSystem S.p.A. in quanto la sua attività non prevede possibili interazioni con gli interessi finanziari dell'Unione Europea			0	nullo
F) INDUZIONE A NON RENDERE DICHIARAZIONI O A RENDERE DICHIARAZIONI MENDACI ALL'AUTORITA' GIUDIZIARIA Art.25-decies D. Lgs. 231/01						
1. Induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria con violenza o minaccia o con offerta o promessa di denaro o di altra utilità	Art.377-bis C.P.	La fattispecie è applicabile in AllSystem S.p.A. dal momento che ha in corso alcuni contenziosi riguardanti prevalentemente cause di lavoro nonché procedimenti penali.	Il personale AllSystem potrebbe venire in contatto ad esempio con soggetti chiamati a testimoniare in un processo e indurli a rendere dichiarazioni mendaci all'autorità giudiziaria in favore della società stessa.	-Direzione Aziendale;	6	medio
				-Area Legale;		
				- Area Risorse Umane prevalentemente in ordine alle cause di lavoro.		
G) DELITTI INFORMATICI E TRATTAMENTO ILLECITO DEI DATI Art. 24-bis D. Lgs. 231/01						

<p>1. Falsità in un documento informatico pubblico o privato avente efficacia probatoria</p> <p>2. Accesso abusivo ad un sistema informatico o telematico</p> <p>3. Detenzione, diffusione e installazione abusiva di apparecchiature, codici e altri mezzi atti all'accesso a sistemi informatici o telematici</p> <p>4. Detenzione, diffusione e installazione abusiva di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico</p> <p>5. Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche e telematiche</p> <p>6. Detenzione, diffusione e installazione abusiva di apparecchiature e di altri mezzi atti a intercettare, impedire o interrompere comunicazioni informatiche o telematiche</p> <p>7. Danneggiamento di informazioni, dati e programmi informatici</p>	<p>Art. 491-bis C.P.</p> <p>Art. 615-ter C.P.</p> <p>Art. 615- quater C.P.</p> <p>Art. 615- quinquies C.P.</p> <p>Art. 617- quater C.P.</p> <p>Art. 617- quinquies C.P.</p> <p>Art. 635-bis C.P.</p>	<p>AllSystem S.p.A. è una società che sviluppa direttamente o tramite società terzi, software proprietari. Detti software tuttavia riguardano prevalentemente la gestione di centrali operative, del parco automezzi, di programmi di rendicontazione ore e fatturazione.</p>	<p>- Si tratta di ipotesi solo astrattamente applicabili in quanto vi sono sistemi di controllo dei log e recupero dei dati che consentirebbero di risalire ad eventuali modifiche di codice o interventi anomali.</p>	<p>- Direzione Aziendale, non direttamente ma per il tramite di personale tecnico;</p>	<p>2</p>	<p>basso</p>
<p>8. Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro Ente Pubblico o comunque di pubblica utilità</p> <p>9. Danneggiamento di sistemi informatici o telematici</p> <p>10. Danneggiamento di sistemi informatici o telematici di pubblica utilità</p> <p>11. Frode informatica del soggetto che presta servizi di certificazione di firma elettronica</p>	<p>Art. 635-ter C.P.</p> <p>Art. 635- quater C.P.</p> <p>Art. 635- quinquies C.P.</p> <p>Art. 640- quinquies C.P.</p>			<p>-Ufficio Tecnico/area CED.</p>		
<p>H) DELITTI DI CRIMINALITA' ORGANIZZATA Art. 24-ter D. Lgs. 231/01</p>						
<p>1. Associazione per delinquere</p> <p>2. Associazioni di tipo mafioso anche straniere (con riguardo a tali ipotesi di reato, la cessione del ramo d'azienda inerente il trasporto e la conta valori intervenuto nel luglio 2020 ha reso parzialmente non attuali le valutazioni che seguono, che tuttavia restano parte</p>	<p>416 comma 6 c.p.</p> <p>416 bis c.p</p>	<p>Si tratta di fattispecie astrattamente ipotizzabili data la partecipazione di AllSystem S.p.A. a gare d'appalto pubbliche o su invito</p>	<p>- Partecipazione ad appalti qualora AllSystem partecipasse ad organizzazioni volte a creare sistemi strutturati di truffa negli appalti pubblici (coinvolgendo ad esempio altre aziende in ATI e/o ponendo in essere sistemi di corruzione di personale di stazioni appaltanti);</p> <p>- Falsificazione di monete ed introduzione delle stesse in circolazione ad esempio partecipando ad associazioni di falsari.</p>	<p>-Direzione Aziendale;</p> <p>- Amministrazione;</p> <p>- Ufficio Gare;</p> <p>- Sale Conta.</p>	<p>7</p> <p>4</p>	<p>alto</p> <p>medio</p>

integrante del modello nel caso in cui la AllSystem decidesse di espandere nuovamente la propria attività)						
3. Scambio elettorale politico-mafioso 4. Sequestro di persona a scopo di rapina o di estorsione 5. Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope 6. Termini di durata massima delle indagini preliminari.	416 ter c.p. 630 c.p. DPR 309/90 407, co. 2, lett. a), numero 5) c.p.p	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.			0	nullo
I) IMPIEGO DI CITTADINI DI PAESI TERZI IL CUI SOGGIORNO È IRREGOLARE Art. 25-duodecies D.Lgs. 231/01						
1. Occupazione di lavoratori stranieri privi del permesso di soggiorno, o con permesso scaduto e non rinnovato, revocato o annullato 2. Procurato ingresso illecito dello straniero nel territorio dello Stato 3. Favoreggiamento della permanenza clandestina dello straniero nel territorio dello Stato	Art. 22 co. 12-bis D.Lgs. 286/1998 Art. 12 commi 3, 3-bis, 3 ter D.Lgs.286/1998 Art. 12 comma 5 D.Lgs.286/1998	La fattispecie è applicabile in AllSystem S.p.A. nel caso di eventuale assunzione di personale dipendente in violazione delle norme sul permesso di soggiorno.	Il rischio in questo caso è praticamente nullo sia perché in AllSystem S.p.A. non sono stati assunti dipendenti o collaboratori stranieri negli ultimi anni ed inoltre un gran numero di dipendenti è rappresentato da Guardie Giurate in cui i controlli sono particolarmente puntuali. C'è inoltre il controllo della documentazione affidato al Consulente del Lavoro ed al successivo Centro per l'Impiego.	Direzione, Area Personale	1	basso
J) REATI AMBIENTALI Art. 25-undecies D.Lgs. 231/01						
1. Inquinamento ambientale 2. Disastro ambientale 3. Delitti colposi contro l'ambiente 4. Traffico e abbandono di materiale ad alta radioattività 5. Circostanze aggravanti 6. Uccisione, distruzione, cattura, prelievo, detenzione di esemplari di specie animali o vegetali selvatiche protette 7. Distruzione o deterioramento di habitat all'interno di un sito protetto 8. Scarichi di acque reflue	Art. 452-bis C.P. Art. 452-quarter C.P. Art. 452-quinquies C.P. Art. 452-sexies C.P. Art. 452-octies C.P. Art. 727 bis C.P. Art. 733 bis C.P. Art. 137	La fattispecie è astrattamente applicabile in AllSystem S.p.A. in quanto l'azienda dispone di una pompa di benzina nella filiale di Milano dismessa da anni.	I rischio risiede nella possibile dispersione di sostanze inquinanti prevalentemente durante: attività di lavaggio delle pompe ed altri eventuali interventi di manutenzione ordinaria; in caso di eventuale manutenzione straordinaria e nella non corretta alimentazione / falsificazione dei registri di carico/scarico.		3	basso

industriali contenenti sostanze pericolose; scarico di sostanze o materiali vietati nelle acque dal mare da parte di navi o aeromobili	D.Lgs. 152/06
9. Attività di gestione di rifiuti non autorizzata	Art. 256 D.Lgs. 152/06
10. Bonifica dei siti	Art. 257 D.Lgs. 152/06
11. Violazione degli obblighi di comunicazione, di tenuta dei registri obbligatori e dei formulari	Art. 258 D.Lgs. 152/06
12. Traffico illecito di rifiuti	Art. 259 D.Lgs. 152/06
13. Attività organizzate per il traffico illecito dei rifiuti (reato abrogato dall'art. 7 co. 1 lett. q) del D.Lgs. 1.03.2018 n. 21 e ora previsto e punito all'art. 452 quaterdecies C.P. ma non rientrante nel catalogo dei reati presupposto)	Art. 260 D.Lgs. 152/06
14. Sistema informatico di controllo della tracciabilità dei rifiuti	Art. 260 bis D.Lgs. 152/06
15. Superamento dei valori limite o delle prescrizioni stabilite nelle autorizzazioni per le emissioni in atmosfera	Art. 279 D.Lgs. 152/06
16. Importazione o esportazione di esemplari di piante appartenenti a specie regolamentate	Art. 1 e 2 L.150/1992
17. Falsificazione o alterazione di certificati, licenze, notifiche di importazione per le specie animali e vegetali protette	Art. 3-bis L.150/1992
18. Detenzione di mammiferi o rettili vivi pericolosi per la salute e l'incolumità pubblica	Art. 6 L. 150/1992
19. Cessazione e riduzione dell'impiego di sostanze lesive	Art. 3 L.549/1993
20. Inquinamento doloso delle acque da parte di navi	Art. 8 D.Lgs. 202/2007
21. Inquinamento colposo delle acque da parte di navi	Art. 9 D.Lgs. 202/2007

K) REATI COMMESSI NEI RAPPORTI CON LA PUBBLICA AMMINISTRAZIONE Art. 24 D. Lgs. 231/01

<p>1. Malversazione a danno dello Stato o di altro Ente Pubblico 2. Indebita percezione di contributi, finanziamenti, o altre erogazioni da parte dello Stato o di altro Ente Pubblico o della Comunità Europea 3. Truffa in danno dello Stato o di altro Ente pubblico o delle Comunità Europee 4. Truffa aggravata per il conseguimento di erogazioni pubbliche 5. Frode informatica in danno dello Stato o di altro Ente Pubblico – sostituzione dell'identità digitale in danno di uno o più soggetti</p>	<p>Art. 316-bis C.P. Art. 316-ter C.P. Art. 640, co.2 n.1 C.P. Art. 640-bis C.P. Art. 640-ter C.P.</p>	<p>Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.</p>			<p>0</p>	<p>nullo</p>
<p>6. Frode nelle pubbliche forniture</p>	<p>Art. 356 C.P.</p>	<p>Il rischio è dovuto alle plurime attività di servizio offerte alle pubbliche amministrazioni (es. servizi di guardiania, piantonamento, portierato ecc.).</p>	<p>L'ipotesi di reato può concretarsi attraverso discrasie create ad arte tra servizi rendicontati e servizi effettivamente effettuati.</p>		<p>6</p>	<p>medio</p>
<p>7. Turbata libertà degli incanti</p>	<p>Art. 353 C.P.</p>	<p>Si tratta di fattispecie astrattamente ipotizzabili data la partecipazione di AllSystem S.p.A. a gare d'appalto pubbliche o su invito</p>			<p>6</p>	<p>medio</p>
<p>8. Turbata libertà del procedimento di scelta del contraente</p>	<p>Art. 353 bis C.P.</p>	<p>Si tratta di fattispecie astrattamente ipotizzabili data la partecipazione di AllSystem S.p.A. a gare d'appalto pubbliche o su invito</p>			<p>6</p>	<p>medio</p>

L) DELITTI CONTRO L'INDUSTRIA E IL COMMERCIO Art. 25.bis1 D. Lgs. 231/01

1. Turbata libertà dell'industria o del commercio	Art. 513 C.P.	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.			0	nullo
2. Illecita concorrenza con minaccia o violenza	Art. 513-bis C.P.					
3. Frodi contro le industrie nazionali	Art. 514 C.P.					
4. Frode nell'esercizio del commercio	Art. 515 C.P.					
5. Vendita di sostanze alimentari non genuine come genuine	Art. 516 C.P.					
6. Vendita di prodotti industriali con segni mendaci	Art. 517 c.p.					
7. Fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale	Art. 517-ter C.P.					
8. Contraffazione di indicazioni geografiche o denominazioni di origine di prodotti agroalimentari	Art. 517- quater C.P.					
M) REATI CON FINALITA' DI TERRORISMO O DI EVERSIONE DELL'ORDINE DEMOCRATICO PREVISTI DAL CODICE PENALE E DALLE LEGGI SPECIALI Art. 25-quater D.Lgs 231/01						
N) PRATICHE DI MUTILAZIONE DEGLI ORGANI GENITALI FEMMINILI Art 25-quarter.1 D.Lgs 231/01						
1. Pratiche di mutilazione degli organi genitali femminili	Art. 583-bis C.P.	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.			0	nullo
O) DELITTI CONTRO LA PERSONALITA' INDIVIDUALE Art. 25-quinquies D.Lgs. 231/01						
1. Riduzione o mantenimento in schiavitù o in servitù	Art. 600 C.P.	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.			0	nullo
1. Prostituzione minorile	Art. 600-bis C.P.					
2. Pornografia minorile	Art. 600-ter C.P.					
3. Detenzione di materiale pornografico	Art. 600.quater C.P.					
4. Pornografia virtuale	Art. 600- quater.1 C.P.					
5. Iniziative turistiche volte allo sfruttamento della prostituzione minorile	Art. 600- quinquies C.P.					
6. Tratta di persone	Art. 601 C.P.					
7. Acquisto o alienazione di schiavi	Art. 602 C.P.					
8. Intermediazione illecita e sfruttamento del lavoro	Art. 603-bis C.P.	L'ipotesi di reato in esame si ritiene concretamente realizzabile in AllSystem S.p.a.			7	alto
P) REATI DI ABUSI DI MERCATO Art. 25-sexies D.Lgs. 231/01						
1. Abuso di informazioni privilegiate	D.Lgs. n.58/1998 art. 184	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.			0	nullo
2. Manipolazione del mercato	D.Lgs. n.58/1998 art. 185					
Q) DELITTI IN MATERIA DI VIOLAZIONE DEL DIRITTO D'AUTORE Art. 25-novies D.Lgs 231/01						
1. Messa a disposizione del pubblico in un sistema di reti telematiche, mediante connessioni di qualsiasi genere e senza averne diritto di un'opera o di parte di un'opera	Art. 171 co. 1 lett. a-bis) L.633/1941	Non si ritengono ragionevolmente applicabili in AllSystem S.p.A.				

dell'ingegno protetta						
2. Reato di cui al punto precedente commesso su un'opera altrui non destinata alla pubblicità, ovvero con usurpazione della paternità dell'opera, ovvero con deformazione, mutilazione o altra modificazione dell'opera stessa, qualora ne risulti offeso l'onore o la reputazione dell'autore	Art. 171 co. 3 L.633/1941					
3. Abusiva duplicazione, per trarne profitto, di programmi per elaboratore; importazione, distribuzione, vendita, detenzione a scopo commerciale e imprenditoriale ovvero concessione in locazione di programmi contenuti in supporti non contrassegnati dalla SIAE; predisposizione di mezzi per consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi di protezione di programmi per elaboratori	Art. 171-bis co. 2 L.633/1941				0	nullo
4. Riproduzione su supporti non contrassegnati SIAE, trasferimento su altro supporto, distribuzione, comunicazione, presentazione o dimostrazione in pubblico del contenuto di una banca dati al fine di trarre profitto; estrazione o reimpiego della banca dati in violazione delle disposizioni sui diritti del costituente e dell'utente di una banca dati; distribuzione, vendita o concessione in locazione di banche di dati	Art. 171-bis co. 2, L. 633/1941					
5. Reati commessi a fini di lucro per uso non personale e caratterizzati da una delle condotte descritte all'art. 171-ter, comma 1, L. 633/1941	Art. 171-ter, comma 1, L. 633/1941					
6. Reati caratterizzati dalle condotte descritte dall' Art. 171-ter comma 2. L. 633/1941	Art. 171-ter comma 2. L. 633/1941					
7. Mancata o falsa comunicazione alla SIAE dei dati per l'identificazione dei supporti non soggetti a contrassegno	Art. 171-septies L. 633/1941					
8. Produzione, messa in vendita, importazione, promozione, installazione, modifica, utilizzo per uso pubblico o privato di apparati o parti di essi atti alla decodificazione di trasmissioni audiovisive e ad accesso condizionato	Art. 171-octies L.633/1941					
R) REATI TRANSNAZIONALI Legge 16 marzo 2006, n.146 art. 3 e 10						

<p>L'art.3 della Legge definisce 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:</p> <p>A. Sia commesso in più di uno Stato;</p> <p>B. ovvero sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato;</p> <p>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;</p> <p>D. ovvero sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato.</p> <p>1. Associazione per delinquere</p> <p>2. Associazione di tipo mafioso</p> <p>3. Associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri</p> <p>4. Associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope</p> <p>5. Disposizioni contro le immigrazioni clandestine</p> <p>6. Introduzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria</p> <p>7. Favoreggiamento personale</p>	<p>Art 416 C.P.</p> <p>Art. 416-bis C.P.</p> <p>Art. 291- quater T.U. di cui al DPR n.43/1973</p> <p>Art. 74 DPR 9 Ottobre 1990, n.309</p> <p>Art. 12 co. 3,3-bis, 3-ter e 5 del T.U. di cui al D.Lgs. n.286/1998</p> <p>Art. 377-bis C.P.</p> <p>Art. 378 C.P.</p>				<p>0</p>	<p>nullo</p>
S) RAZZISMO E XENOFOBIA Art. 25-terdecies D.Lgs. 231/01						
<p><u>Art. 3, comma 3 bis L.13 ottobre 1975 n. 654</u> (articolo abrogato dall'art. 7, comma 1, lettera c), del D.Lgs. 1° marzo 2018, n. 21. Vedi l'articolo 604-bis del codice penale inserito dall'art. 2, comma 1, lett. i), D.Lgs. 1° marzo 2018, n. 21 e attualmente non risulta richiamato nel catalogo dei reati presupposto previsti dall'Art. 25-terdecies D. Lgs. 8 giugno 2001, n. 231).</p>						
T) FRODE IN COMPETIZIONI SPORTIVE, ESERCIZIO ABUSIVO DI GIOCO O DI SCOMMESSA E GIOCHI D'AZARDO ESERCITATI A MEZZO DI APPARECCHI VIETATI Art. 25-quaterdecies D.Lgs. 231/01						
<p>1. Frode in competizioni sportive;</p> <p>2. Esercizio abusivo di attività di giuoco o di scommessa</p>	<p>Artt. 1 e 4 Legge 13 dicembre</p>	<p>Le ipotesi di reato in esame non si ritengono ragionevolmente realizzabili in</p>			<p>0</p>	<p>nullo</p>

	1989 n. 401	AllSystem S.p.a.				
U) REATI TRIBUTARI Art. 25-quinquiesdecies D.Lgs. 231/01						
1. Dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti	Art. 2 D.Lgs. n. 74/2000	La fattispecie è applicabile in AllSystem S.p.A. in quanto la stessa nell'ambito della propria attività si avvale di molteplici fornitori, sebbene ogni fornitura sia debitamente contrattualizzata.			4	medio
2. Dichiarazione fraudolenta mediante altri artifici	Art. 3 D.Lgs. n. 74/2000	La fattispecie è applicabile in AllSystem S.p.A. in quanto la stessa nell'ambito della propria attività si avvale di molteplici fornitori, sebbene ogni fornitura sia debitamente contrattualizzata.			4	medio
3. Emissione di fatture o altri documenti per operazioni inesistenti	Art. 8 D.Lgs. n. 74/2000	La fattispecie è applicabile in AllSystem S.p.A. in particolare in relazione a servizi resi in favore di soggetti privati			6	medio
4. Occultamento o distruzione di documenti contabili	Art. 10 D.Lgs. n. 74/2000	La fattispecie è applicabile in AllSystem S.p.A.			2	basso
5. Sottrazione fraudolenta al pagamento di imposte	Art. 11 D.Lgs. n. 74/2000	L'ipotesi di reato in esame non si ritengono ragionevolmente realizzabili in AllSystem S.p.a.			0	nullo
6. Dichiarazione infedele (quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'U.E., da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro)	Art. 4 D.Lgs. n. 74/2000	L'ipotesi di reato in esame non si ritiene ragionevolmente realizzabile in AllSystem S.p.a.			0	nullo
7. Omessa dichiarazione (quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'U.E., da cui consegua o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro)	Art. 5 D.Lgs. n. 74/2000	L'ipotesi di reato in esame non si ritiene ragionevolmente realizzabile in AllSystem S.p.a.			0	nullo

8. Indebita compensazione (quando sono commessi al fine di evadere l'imposta sul valore aggiunto nell'ambito di sistemi fraudolenti transfrontalieri connessi al territorio di almeno un altro Stato membro dell'U.E., da cui consegue o possa conseguire un danno complessivo pari o superiore a dieci milioni di euro)	Art. 10- quater D.Lgs. n. 74/2000	L'ipotesi di reato in esame non si ritiene ragionevolmente realizzabile in AllSystem S.p.a.			0	nullo
V) CONTRABBANDO Art. 25-sexiesdecies D.Lgs. 231/01						
1. Contrabbando	D.P.R. 23 gennaio 1973 n. 43 (T.U. Disposizioni legislative in materia doganale	Le ipotesi di reato in esame non si ritengono ragionevolmente realizzabili in AllSystem S.p.a.			0	nullo
Z) DELITTI IN MATERIA DI STRUMENTI DI PAGAMENTO DIVERSI DAI CONTANTI E TRASFERIMENTO FRAUDOLENTO DI VALORI Art. 25-octies1 D.Lgs. 231/01						
1. Indebito utilizzo e falsificazione di strumenti di pagamento diversi dai contanti	Art. 493-ter C.P.	Le ipotesi di reato in esame non si ritengono ragionevolmente realizzabili in AllSystem S.p.a.			0	nullo
2. Detenzione e diffusione di apparecchiature, dispositivi o programmi informatici diretti a commettere reati riguardanti strumenti di pagamento diversi dai contanti	Art. 493- quater C.P.					
3. Trasferimento fraudolento di valori	Art. 512-bis C.P.	Le ipotesi di reato in esame si ritengono astrattamente realizzabili in AllSystem S.p.a. in quanto utilizza per il pagamento delle forniture di beni di servizi l'internet banking (bonifici), una carta di credito in uso alla sola area Amministrazione nonché carte carburante.			1	basso
4. Frode informatica	Art. 640-ter, co. 2 C.P.					
AA) DELITTI CONTRO IL PATRIMONIO CULTURALE Art. 25-septiesdecies D.Lgs. 231/01						
1. Furto di beni culturali	Art. 518-bis C.P.	Le ipotesi di reato in esame si ritengono astrattamente realizzabili in AllSystem S.p.a. in quanto svolge servizi di vigilanza e sorveglianza presso enti museali o comunque presso soggetti (pubblici e privati) ove sono custoditi beni			4	medio
2. Appropriazione indebita di beni culturali	Art. 518-ter C.P.					
3. Ricettazione di beni culturali	Art. 518- quater C.P.					
4. Falsificazione in scrittura privata relativa a beni culturali	Art. 518- octies C.P.					
5. Violazioni in materia di alienazione di beni culturali	Art. 518 novies C.P.					

6. Importazione illecita di beni culturali	Art. 518-decies C.P.	culturali				
7. Uscita o esportazione illecite di beni culturali	Art. 518-undecies C.P.					
8. Distruzione, dispersione, deterioramento, deturpamento, imbrattamento e uso illecito di beni culturali o paesaggistici	Art. 518-duodecies C.P.					
9. Contraffazione di opere d'arte	Art. 518-quaterdecies C.P.					
AB) RICICLAGGIO DI BENI CULTURALI E DEVASTAZIONE E SACCHEGGIO DI BENI CULTURALI E PAESAGGISTICI Art. 25-duodecies D.Lgs. 231/01						
1. Riciclaggio di beni culturali	Art. 518-sexies C.P.	Le ipotesi di reato in esame si ritengono astrattamente realizzabili in AllSystem S.p.a. in quanto svolge servizi di vigilanza e sorveglianza presso enti museali o comunque presso soggetti (pubblici e privati) ove sono custoditi beni culturali			4	medio
2. Devastazione e saccheggio di beni culturali e paesaggistici	Art. 518-terdecies C.P.					