MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL D. LGS. 231/2001

DI

CONSIP S.P.A. a socio unico

Versione approvata dal Consiglio di Amministrazione in data 11 febbraio 2021

Sommario

DEFINIZIONI 6
CAPITOLO 1 DESCRIZIONE DEL QUADRO NORMATIVO 9
1.1 Il decreto legislativo n. 231 dell'8 giugno 2001 9
1.2 Le fattispecie di reato richiamate dal Decreto 10
1.3 Presupposti per l'imputazione all'ente della responsabilità amministrativa 16
1.3.a) Criteri di imputazione oggettivi e soggettivi 16
1.3.b) Reato-presupposto commesso da soggetti apicali 16
1.3.c) Reato-presupposto commesso da soggetti sottoposti 17
1.4 Le sanzioni previste dal Decreto 18
1.5 Requisiti del Modello - Le Linee Guida emanate dall'associazione di categoria (Confindustria) e Circolare n. 83607/2012 della Guardia di Finanza 19
CAPITOLO 2 LA STRUTTURA ORGANIZZATIVA ED AZIENDALE DI CONSIP SpA 22
2.1 Le attività 22
2.2 Corporate Governance 23
2.3 Organizzazione interna e struttura organizzativa 24
2.4 Sistema deleghe 26
2.5 Sistema dei controlli 27
2.5.a) Controlli di Linea - I livello -permanenti 28
2.5.b) Controlli di II Livello - permanenti 28
2.5.c) Controllo di III livello - periodico 34
2.5.d) Ulteriori controlli 34
2.6 Mappatura dei processi 35
CAPITOLO 3 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI CONSIP SpA 40
3.1 Premessa: le azioni poste in essere da Consip e i principi ispiratori 40
3.2 Il Modello di organizzazione, gestione e controllo ex d.lgs. n. 231/2001 e il Piano anticorruzione 42
3.3 Struttura del Modello 43
3.3.a) Struttura della Parte Generale 43
3.3.b) Struttura delle Parti Speciali 44
3.4 Rilievi preliminari sulle principali aree di esposizione di Consip ai rischi di commissione di reati-presupposto 45
3.5 Il Codice Etico 46
3.6 Termini e modalità di adozione e di aggiornamento del Modello e del Codice Etico da parte degli organi di vertice 47
3.6.a) Gruppo di lavoro 47
3.6.b) Adozione del Modello da parte degli Organi di Vertice 48
3.6.c) Modalità di aggiornamento 48
3.6.d) Comunicazione e pubblicazione del Modello e/o del Codice Etico 50
3.7 I Destinatari e i Referenti del Modello 50
3.7.a) Destinatari 50
3.7.b) Principi di comportamento dei Destinatari 51
3.7.c) Referenti 51
CAPITOLO 4 GESTIONE DEL RISCHIO 53
4.1 Risk assessment integrato 53

4.2 Famiglie di rischio ... 55
4.3 Individuazione delle aree a rischio e dei rischi specifici ... 55
4.3.a) Individuazione delle aree a rischio ... 55
4.3.b) Identificazione dei rischi ... 56
4.5 Valutazione dei rischi ... 59
4.5.a) Metodologia di Valutazione del Rischio Inerente ... 60
4.5.b) Metodologia di Valutazione Presidi di Controllo ... 62
4.5.c) Metodologia Valutazione Rischio Residuo ... 63
4.5.d) Rischiosità complessiva media e per processo ... 64
4.5.e) Rischiosità complessiva per Famiglia di Rischio ... 64
4.5.f) Fattori abilitanti, conseguenze, anomalie significative e indicatori di rischio ... 65
4.6 Trattamento dei rischi ... 65
4.7 Misure preventive di controllo del rischio generali ... 66
CAPITOLO 5 L'ORGANISMO DI VIGILANZA ... 73
5.1 Caratteristiche generali dell'Organismo di Vigilanza della Società ... 73
5.1.a) Caratteristiche ... 73
5.1.b) Requisiti di professionalità ... 74
5.1.c) Requisiti di onorabilità ... 74
5.2 Nomina dell'OdV ... 75
5.3 Decadenza e sostituzione dei componenti dell'OdV ... 76
5.4 Funzioni, poteri e compiti dell'OdV ... 76
5.5 Reporting e flussi ... 78
5.5.a) Reporting dell'Organismo di Vigilanza ed incontri periodici ... 78
5.5.b) Rapporti tra OdV e altri organi di controllo ... 79
5.5.c) Reporting vs l'OdV ... 79
5.5.d) Flussi vs il RPCT e OdV ... 80
CAPITOLO 6 WHISTLEBLOWING ... 81
6.1 Contesto normativo ... 81
6.2 Il Sistema di whistleblowing ... 83
6.2.a) Sistema adottato ... 83
6.2.b) Accesso al Sistema ... 84
6.2.c) Gestione delle segnalazioni ... 84
6.3 Segnalazioni provenienti da utenti registrati ... 87
6.4 Segnalazioni anonime ... 87
6.5 Tutela del whistleblower ... 88
6.5.a) Tutela dell'identità del segnalante ... 88
6.5.b) Divieto di discriminazione ... 89
6.5.c) Sottrazione al diritto di accesso ... 90
6.5.d) Distacco o casi analoghi ... 90
CAPITOLO 7 MONITORAGGIO E CONTROLLI ... 91
7.1 Piano Integrato dei Controlli ... 91
7.2 Attività istruttoria sulle segnalazioni ... 92
CAPITOLO 8 DIFFUSIONE ED AGGIORNAMENTO DEL MODELLO ... 96
8.1 Formazione ... 96
8.1.a) Piano di formazione integrato ... 96
8.1.b) Discenti ... 97
8.2. Comunicazione e pubblicazione del Modello e/o del Codice Etico ... 97
8.3 Informazione ai soggetti terzi ... 97

CAPITOLO 9 IL SISTEMA DISCIPLINARE 99
9.1 Il Sistema disciplinare 99

ALLEGATI

PARTI SPECIALI

- A Reati contro la Pubblica Amministrazione
- B Delitti informatici
- C Reati Societari
- D Reati in materia di sicurezza e salute sul lavoro
- E Reati di ricettazione, riciclaggio e impiego di danaro, beni o utilità di provenienza illecita
- F Reati di Abusi di Mercato
- G Reati transnazionali
- H Delitti di Criminalità Organizzata
- K Delitti contro l'industria ed il commercio
- I Delitti in violazione del Diritto d'Autore
- L Reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'Autorità Giudiziaria
- M Reato di impiego di cittadini di Paesi terzi il cui soggiorno è irregolare
- N Reati Ambientali
- O Reati di istigazione al razzismo e xenofobia
- P Reati tributari

SCHEDE RISCHIO

MATRICE DELLA ATTIVITÀ A RISCHIO REATO / REFERENTI

CODICE ETICO

SISTEMA DISCIPLINARE

Matrice delle revisioni

1^ edizione: in vigore dal 13 ottobre 2003

2^ edizione: in vigore dal 25 marzo 2005

3^ edizione: in vigore dal 11 aprile 2005

4^ edizione: in vigore dal 27 settembre 2005

5^ edizione: in vigore dal 26 luglio 2010

6^ edizione: in vigore dal 21 giugno 2011

7^ edizione: in vigore dal 18 aprile 2012

8^ edizione: in vigore dal 17 dicembre 2012

9^ edizione: in vigore dal 30 luglio 2014

10^ edizione: in vigore dal 14 aprile 2015

11^ edizione: in vigore dal 18 dicembre 2015

12^ edizione: in vigore dal 14 febbraio 2017

DEFINIZIONI

PRESIDENTE: il Presidente della Società;

AMMINISTRATORE DELEGATO: l'Amministratore Delegato della Società;

AREE A RISCHIO: le aree di attività nel cui ambito risulta profilarsi, in termini più concreti, il rischio di commissione dei reati;

ATTIVITÀ SENSIBILI o ATTIVITA' A RISCHIO: attività aziendali nello svolgimento della quale potrebbe presentarsi il rischio di commissione di uno dei reati espressamente richiamati dal Decreto;

C.C.N.L.: il Contratto Collettivo Nazionale di Lavoro di Consip S.p.A.;

CODICE ETICO: il Codice Etico di Consip S.p.A., che contiene i principi generali di comportamento - ovvero, raccomandazioni, obblighi e/o divieti - a cui i Destinatari devono attenersi e la cui violazione è sanzionata, approvato dal Consiglio di Amministrazione;

CONTRIBUTOR: colui che, sebbene non in via prevalente e significativa come il risk owner (i) contribuisce a prevenire il rischio e a garantire che il rischio sia gestito in modo appropriato, (ii) può incidere sull'attività rilevata;

DECRETO: il Decreto Legislativo 8 giugno 2001, n. 231 e successive modifiche, recante la *"Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300"*, pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e successive modificazioni ed integrazioni (di seguito Decreto);

DESTINATARI: membri degli Organi Sociali, Lavoratori subordinati (Dirigenti e impiegati), lavoratori autonomi, collaboratori esterni, e tutti coloro con cui Consip S.p.A. si relaziona nello svolgimento delle attività aziendali;

DIPENDENTI: tutte le persone fisiche che intrattengono con Consip S.p.A. un rapporto di lavoro subordinato;

DP: Dirigente preposto alla redazione dei documenti contabili societari nominato da Consip S.p.A.;

ENTE nell'ambito del Modello ex D.Lgs. 231/2001, soggetto al quale riferire la responsabilità amministrativa per reati commessi nel suo interesse o vantaggio da persone fisiche;

FORNITORI: i fornitori di beni e/o servizi e/o lavori di Consip S.p.A.;

INCARICATI DI UN PUBBLICO SERVIZIO: ai sensi dell'art. 358 c.p. "*sono incaricati di un pubblico servizio coloro i quali, a qualunque titolo, prestano un pubblico servizio. Per pubblico servizio deve intendersi un'attività disciplinata nelle stesse forme della pubblica funzione, ma caratterizzata dalla mancanza dei poteri tipici di quest'ultima, e con esclusione dello svolgimento di semplici mansioni di ordine e della prestazione di opera meramente materiale*";

INTERESSE: finalità – anche non esclusiva - della condotta illecita, consistente nel favorire l'Ente, che deve essere accertata *ex ante* e che sussiste a prescindere dal conseguimento effettivo dell'obiettivo;

LINEE GUIDA: le Linee Guida adottate da Confindustria per la predisposizione dei modelli di organizzazione, gestione e controllo ai sensi dell'art. 6, comma 3, del d.lgs. 231/2001;

MODELLO - MOG: "Modello di organizzazione, gestione e controllo" adottato da Consip S.p.A., ai sensi del d.lgs. 231/2001;

ORGANI SOCIALI: il Consiglio di Amministrazione, il Collegio Sindacale e l'Assemblea degli Azionisti della Società;

ORGANISMO DI VIGILANZA (ODV): l'Organismo nominato ai sensi dell'art. 6 del Decreto e avente il compito di vigilare sull'adeguatezza e sull'osservanza del Modello di organizzazione, gestione e controllo, nonché sull'aggiornamento dello stesso;

PERSONALE APICALE: i soggetti di cui all'articolo 5, comma 1, lett. a) del Decreto, ovvero i soggetti che rivestono funzioni di rappresentanza, di amministrazione o di direzione della Società o di una sua Divisione organizzativa dotata di autonomia finanziaria e funzionale o che esercitano, anche di fatto, la gestione e il controllo della Società; in particolare, i membri del Consiglio di Amministrazione, il Presidente, i responsabili di Divisione e di Area e gli eventuali institori e procuratori della Società;

PERSONALE SOTTOPOSTO AD ALTRUI DIREZIONE: i soggetti di cui all'articolo 5, comma 1, lett. b) del Decreto, ovvero tutto il personale che opera sotto la direzione o la vigilanza del personale apicale;

PROTOCOLLI DI PREVENZIONE: protocolli diretti a programmare la formazione e l'attuazione delle decisioni dell'Ente in relazione ai reati da prevenire;

PTPC: Piano triennale per la prevenzione della corruzione e della trasparenza adottato da Consip S.p.A.;

PUBBLICA AMMINISTRAZIONE: l'insieme degli enti pubblici (es. amministrazioni pubbliche) che concorrono all'esercizio ed alle funzioni dell'amministrazione dello Stato nelle materie di sua competenza;

PUBBLICI UFFICIALI: ai sensi dell'art. 357 c.p. "*sono pubblici ufficiali coloro i quali esercitano una pubblica funzione legislativa, giudiziaria o amministrativa. Agli stessi effetti è pubblica la funzione amministrativa disciplinata da norme di diritto pubblico e da atti autoritativi, e caratterizzata dalla formazione e dalla manifestazione della volontà della pubblica amministrazione o dal suo svolgersi per mezzo di poteri autoritativi o certificativi";*

REATI PRESUPPOSTO: gli specifici reati individuati dal Decreto da cui può derivare la responsabilità amministrativa dell'Ente;

REFERENTE: responsabili delle Divisioni aziendali coinvolte in ciascuna area a rischio-reato individuata sono responsabili dell'effettiva applicazione delle attività di controllo poste in essere per la prevenzione dei reati previsti dal Decreto

RISCHIO DI REATO: riferito al rischio di commissione di uno dei reati considerati dal decreto;

RISK OWNER: colui che (i) è titolato a prevenire il rischio e a garantire che il rischio sia gestito in modo appropriato, ovvero (ii) che ha la possibilità di incidere significativamente sull'attività rilevata, sia da solo che in accordo con altri;

RPCT: Responsabile della prevenzione della corruzione e della trasparenza nominato da Consip S.p.A.

SCI: Sistema Controlli Interni

SOCIETÀ: Consip S.p.A.

VANTAGGIO: risultato positivo, non necessariamente economico, che l'Ente ha obiettivamente tratto a prescindere dall'intenzione di chi ha commesso l'illecito e che deve essere accertato *ex post.*

CAPITOLO 1
DESCRIZIONE DEL QUADRO NORMATIVO

1.1 IL DECRETO LEGISLATIVO N. 231 DELL'8 GIUGNO 2001

Il Decreto Legislativo n. 231 datato 8 giugno 2001 (recante la "*Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'art. 11 della legge 29 settembre 2000, n. 300*", pubblicato in Gazzetta Ufficiale n. 140 del 19 giugno 2001, e le sue successive modificazioni e/o integrazioni: il "**Decreto**")[1] ha introdotto nell'ordinamento giuridico italiano la c.d. "responsabilità amministrativa" degli enti, anche privi di personalità giuridica, con esclusione dello Stato, degli enti pubblici territoriali, degli enti che svolgono funzioni di rilievo costituzionale e degli enti pubblici non economici.

La responsabilità dell'Ente consegue al verificarsi di determinati **illeciti penali** (c.d. Reati presupposto), tassativamente previsti dallo stesso Decreto, **commessi nell'interesse o vantaggio dell'Ente**, da coloro che:

a) rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'Ente o di una sua unità organizzativa dotata di autonomia finanziaria e funzionale;
b) esercitano, anche di fatto, la gestione e il controllo dello stesso Ente;
c) sono sottoposti alla direzione o alla vigilanza di uno dei soggetti sopra elencati.

E' escluso, pertanto, che si configuri un'ipotesi di responsabilità nei casi in cui l'autore abbia commesso il reato nell'esclusivo interesse proprio o di terzi.

Tale responsabilità si colloca tra il sistema amministrativo e il sistema penale, introducendo così nell'ordinamento giuridico un vero e proprio "*tertium genus*"[2] di responsabilità che si fonda sui principi cardine di quest'ultimo, sia sul piano processuale che sul piano sostanziale, rilevando i principi di legalità - con tutti i suoi corollari, ovvero riserva di legge, irretroattività, tassatività, divieto di analogia ed offensività - ed il principio di colpevolezza.

La Società risponde per "colpa di organizzazione" (cfr. successivo § 1.3) in via amministrativa (con le modalità del diritto e del processo penale) per non aver predisposto e attuato un sistema di

[1] La legge 300/2000 ha ratificato ed eseguito diverse convenzioni internazionali 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).

In relazione alla ratifica delle convenzioni sopra citate (per lo più elaborate in base all'art. K.3 del Trattato dell'Unione europea), la legge 300/2000 conteneva la delega al Governo per la disciplina della responsabilità amministrativa delle persone giuridiche e degli enti privi di personalità giuridica: disciplina necessaria in quanto, fra gli obblighi convenzionali assunti dall'Italia vi era, anche, l'introduzione di una responsabilità degli enti collettivi.

[2] Relazione ministeriale al D. Lgs. 231/01.

organizzazione, gestione e controllo diretto a monitorare i processi critici con l'intento e lo scopo di prevenire la commissione di fattispecie criminose.

La responsabilità amministrativa della Società non sostituisce quella personale del soggetto che ha commesso il reato ma si affianca a questa; l'art. 8 del Decreto afferma in proposito che la responsabilità della Società sussiste anche quando:

- l'autore del reato non è stato identificato o non è imputabile;
- il reato si estingue per una causa diversa dall'amnistia.[3]

1.2 LE FATTISPECIE DI REATO RICHIAMATE DAL DECRETO

L'ente, dunque, può essere ritenuto responsabile solo con riguardo ai reati-presupposto, se commessi nel suo interesse o a suo vantaggio dai soggetti qualificati *ex* art. 5, comma 1, del Decreto. I reati-presupposto possono essere compresi, per comodità espositiva, nelle seguenti categorie:

a. delitti contro la Pubblica Amministrazione, richiamati dagli artt. 24 e 25 del Decreto[4];

[3] Non si procede nei confronti della società quando l'amnistia è concessa per un reato in relazione al quale è prevista la sua responsabilità e l'imputato ha rinunciato alla sua applicazione.

[4] Si tratta dei reati seguenti: malversazione a danno dello Stato o dell'Unione europea (art. 316-*bis* c.p.), indebita percezione di erogazioni a danno dello Stato (art. 316-*ter* c.p.), truffa aggravata a danno dello Stato (art. 640, comma 2, n. 1, c.p.), truffa aggravata per il conseguimento di erogazioni pubbliche (art. 640-*bis* c.p.), frode informatica a danno dello Stato o di altro ente pubblico (art. 640-*ter* c.p.), corruzione per l'esercizio della funzione (art. 318 c.p.), corruzione per un atto d'ufficio o contrario ai doveri d'ufficio (artt. 319 e 319-*bis* c.p.), corruzione di persona incaricata di un pubblico servizio (art. 320 c.p.), corruzione in atti giudiziari (art. 319-*ter* c.p.), induzione indebita a dare o promettere utilità (art. 319 – quater), istigazione alla corruzione (art. 322 c.p.), concussione (art. 317 c.p.), peculato, corruzione e istigazione alla corruzione di membri degli organi delle Comunità europee e di funzionari delle Comunità europee e di degli Stati esteri (art. 322-*bis* c.p.), traffico di influenze illecite (art. 346-*bis* c.p.). La Legge n. 69/2015 recante *"Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio"* ha introdotto un inasprimento del trattamento repressivo e sanzionatorio dei reati contro la PA, in particolare per quanto riguarda i delitti di corruzione, concussione e peculato. La disciplina sanzionatoria vede aumentare le pene minime e massime per molti illeciti tra cui i reati di corruzione, di abuso di ufficio e di peculato. Per quanto riguarda il reato di concussione, la nuova legge estende il novero dei soggetti perseguibili anche all'incaricato di pubblico servizio oltre che al pubblico ufficiale. La Legge n. 3/2019 recante "*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* "(c.d "*Legge Spazzacorrotti"),* introdotto delle modifiche al reato di cui all'art. 346 *bis*, c.p., rubricato "*Traffico di influenze illecite*", attualmente inserito tra i reati presupposto della responsabilità dell'ente. Con la predetta legge sono inoltre state inasprite le sanzioni interdittive, previste dall'art. 9, d.lgs. 231/2001 per i reati contro la P.A.; infatti, il nuovo comma 5 dell'art. 25, d.lgs. 231/2001 aumenta nettamente la durata delle sanzioni interdittive per i reati di concussione (art. 317, c.p.), corruzione propria (art. 319, c.p.), corruzione in atti giudiziari (art. 319-ter, c.p.), induzione indebita a dare o promettere utilità (art. 319-quater, c.p.), istigazione alla corruzione propria (art. 322, commi 2 e 4, c.p.), operando anche una distinzione tra reato commesso dal soggetto apicale e reato commesso dal soggetto "sottoposto": nel primo caso, la durata delle interdittive sarà compresa tra 4 e 7 anni; nel secondo caso, tra 2 e 4 anni. Con il D. lgs. del 14 luglio 2020 n. 75, recante l'attuazione della direttiva UE 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'UE mediante il diritto penale, sono state introdotte modifiche ai reati di cui agli artt. 316 (Peculato mediante profitto dell'errore altrui); 316 ter (Indebita percezione di erogazioni a danno dello Stato); 319 quater (induzione indebita a dare o promettere utilità); 322bis (Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e istigazione alla corruzione di membri delle Corti internazionali o degli organi delle Comunità europee o di assemblee parlamentari internazionali o di organizzazioni internazionali e di funzionari delle Comunità europee e di Stati esteri) e 640 (Truffa). Le modifiche introdotte riguardano per lo più la previsione dell'ipotesi che il fatto/reato commesso offenda gli interessi finanziari dell'Unione europea e conseguente previsione della relativa pena per tale fattispecie di reato.

b. delitti informatici e trattamento illecito di dati, richiamati dall'art. 24-*bis* del Decreto[5];

c. delitti di criminalità organizzata, richiamati dall'art. 24-*ter* del Decreto [6];

d. delitti di falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento, richiamati dall'art. 25-*bis* del Decreto [7];

Inoltre il D. lgs. Del 14 luglio 2020 n. 75, recante l'attuazione della direttiva UE 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'UE mediante il diritto penale ha apportato modifiche agli articoli 24 e 25 del D.lgs 231/2001. In particolare all'articolo 24:
1) la rubrica è sostituita dalla seguente: «Indebita percezione di erogazioni, truffa in danno dello Stato, di un ente pubblico o dell'Unione europea o per il conseguimento di erogazioni pubbliche, frode informatica in danno dello Stato o di un ente pubblico e frode nelle pubbliche forniture.»;
2) al comma 1 dopo le parole: «316 -*ter* ,» è inserita la seguente «356,» e dopo le parole: «ente pubblico» sono inserite le seguenti: «o dell'Unione europea»;
3) dopo il comma 2, è inserito il seguente: «2 -*bis* .Si applicano all'ente le sanzioni previste ai commi precedenti in relazione alla commissione del delitto di cui all'articolo 2 della legge 23 dicembre 1986, n. 898.»
Mentre all'art. 25 sono apportate le seguenti modifiche:
1) la rubrica è sostituita dalla seguente: «Peculato, concussione, induzione indebita a dare o promettere utilità, corruzione e abuso d'ufficio.»;
2) al comma 1 è aggiunto, in fine, il seguente periodo: «La medesima sanzione si applica, quando il fatto offende gli interessi finanziari dell'Unione europea, in relazione alla commissione dei delitti di cui agli articoli 314, primo comma, 316 e 323 del codice penale.»
Con riferimento al sopra richiamato reato di cui all'art 323 c.p. "abuso d'ufficio" si segnala che il Decreto Legge n. 76 del 16 luglio 2020 " Decreto Semplificazioni" tra le varie modifiche all'ordinamento vigente ha innovato il predetto reato sostituendo nell'articolato le parole "violazione di norme di legge o regolamento" con "*violazione di specifiche regole di condotta espressamente previste dalla legge o da atti aventi forza di legge e dalle quali non residuino margini di discrezionalità*" restringendo le condotte penalmente rilevanti ai sensi dell'art. 323 c.p. e limitando l'abuso penalmente rilevante alla violazione di specifiche ed espresse regole di condotta; escludendo così l'integrazione del reato di abuso di ufficio in caso di violazione di principi generali.

[5] L'art. 24-*bis* è stato introdotto nel d.lgs. 231/2001 dall'art. 7 della legge 18 marzo 2008, n. 48. Si tratta dei reati di falsità, uso di atti falsi, soppressione, distruzione e occultamento di atti veri e copie autentiche che tengono luogo degli originali mancanti, riguardanti un documento informatico pubblico o privato avente efficacia probatoria (art. 491-*bis* c.p.), accesso abusivo ad un sistema informatico o telematico (art. 615-*ter* c.p.), detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 615-*quater* c.p.), diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico (art. 615-*quinquies* c.p.), intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 617-*quater* c.p.), installazione d'apparecchiature per intercettare, impedire od interrompere comunicazioni informatiche o telematiche (art. 617-*quinquies* c.p.), danneggiamento di informazioni, dati e programmi informatici, nonché di sistemi informatici o telematici (artt. 635-*bis*, 635-*ter*, 635-*quater*, 635-*quinquies* c.p.) e frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-*quinquies* c.p.).

[6] L'art. 24-*ter* è stato introdotto nel d.lgs. 231/2001 dall'art. 2 della legge 15 luglio 2009, n. 94. Si tratta dei reati di associazione per delinquere (art. 416 c.p.), dei reati previsti dall'art. 12 d.lgs. 25 luglio 1998, n. 286 sulle disposizioni in materia di immigrazioni clandestine, dei delitti commessi avvalendosi delle condizioni di cui all'art. 416-*bis* c.p. sulle associazioni di stampo mafioso (la Legge n. 69/2015 recante "disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio" ha introdotto all'art. 5 anche un inasprimento delle pene previste per il reato di associazione di tipo mafioso), di scambio elettorale politico-mafioso (art. 416-*ter* c.p.), sequestro di persona a scopo di rapina o di estorsione (art. 630 c.p.), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 d.p.r. 9 ottobre 1990, n. 309), produzione, traffico e detenzione illeciti di sostanze stupefacenti o psicotrope *(*art. 73 d.p.r. 9 ottobre 1990, n. 309).

[7] L'art. 25-*bis* è stato introdotto nel d.lgs. 231/2001 dall'art. 6 del D.L. 350/2001, convertito in legge, con modificazioni, dall'art. 1 della L. 409/2001; in seguito, esso è stato modificato dall'art. 15 della L. 99/2009. Si tratta dei reati di falsificazione di monete, spendita e introduzione nello Stato, previo concerto, di monete falsificate (art. 453 c.p.), alterazione di monete (art. 454 c.p.), spendita e introduzione nello Stato, senza concerto, di monete falsificate (art. 455 c.p.), spendita di monete falsificate ricevute in buona fede (art. 457 c.p.), falsificazione di valori di bollo, introduzione nello Stato, acquisto, detenzione o messa in circolazione di valori di bollo falsificati (art. 459 c.p.), contraffazione di

e. delitti contro l'industria e il commercio, richiamati dall'art. 25-*bis.1* del Decreto[8];

f. reati societari, richiamati dall'art. 25-*ter* del Decreto[9];

g. delitti in materia di terrorismo e di eversione dell'ordine democratico, richiamati dall'art. 25-*quater* del Decreto [10];

h. pratiche di mutilazione degli organi genitali femminili, richiamati dall'art. 25-*quater1* del Decreto [11];

---

carta filigranata in uso per la fabbricazione di carte di pubblico credito o di valori di bollo (art. 460 c.p.), fabbricazione o detenzione di filigrane o di strumenti destinati alla falsificazione di monete, di valori di bollo o di carta filigranata (art. 461 c.p.), uso di valori di bollo contraffatti o alterati (art. 464 c.p.), contraffazione, alterazione o uso di marchi o segni distintivi ovvero di brevetti, modelli e disegni (art. 473 c.p.), introduzione nello Stato e commercio di prodotti con segni falsi (art. 474 c.p.).

[8] L'art. 25-*bis.1* è stato introdotto nel d.lgs. 231/2001 dall'art. 15 della L. 99/2009. Si tratta dei reati di turbata libertà dell'industria o del commercio (art. 513 c.p.), illecita concorrenza con minaccia o violenza (art. 513-*bis* c.p.), frodi contro le industrie nazionali (art. 514 c.p.), frode nell'esercizio del commercio (art. 515 c.p.), vendita di sostanze alimentari non genuine come genuine (art. 516 c.p.), vendita di prodotti industriali con segni mendaci (art. 517 c.p.), fabbricazione e commercio di beni realizzati usurpando titoli di proprietà industriale (art. 517-*ter* c.p.), contraffazione di indicazioni geografiche o denominazioni di origine dei prodotti agroalimentari (art. 517-*quater* c.p.).

[9] L'art. 25-*ter* è stato introdotto nel d.lgs. 231/2001 dall'art. 3 del d.lgs.61/2002. Si tratta dei reati di false comunicazioni sociali e false comunicazioni sociali in danno dei soci o dei creditori (artt. 2621 e 2622 c.c.), falso in prospetto (art. 2623 c.c.), impedito controllo (art. 2625, comma 2, c.c.), formazione fittizia del capitale (art. 2632 c.c.), indebita restituzione dei conferimenti (art. 2626 c.c.), illegale ripartizione degli utili e delle riserve (art. 2627 c.c.), illecite operazioni sulle azioni o quote sociali o della società controllante (art. 2628 c.c.), operazioni in pregiudizio dei creditori (art. 2629 c.c.), indebita ripartizione dei beni sociali da parte dei liquidatori (art. 2633 c.c.), illecita influenza sull'assemblea (art. 2636 c.c.), aggiotaggio (art. 2637 c.c.), ostacolo all'esercizio delle funzioni delle autorità pubbliche di vigilanza (art. 2638 c.c.).La legge 6 novembre 2012, n. 190 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione", c.d. legge anticorruzione (pubblicata in G.U. n. 265 del 13 novembre 2012) ha introdotto nel catalogo dei reati presupposto la corruzione tra privati (art. 2635 e 2635-bis c.c.). La Legge n. 69/2015 recante "Disposizioni in materia di delitti contro la Pubblica Amministrazione, di associazioni di tipo mafioso e di falso in bilancio" ha inoltre modificato il reato di false comunicazioni sociali qualificandolo non più come contravvenzione bensì come delitto e rinvia al modificato art. 2621 c.c. che introduce la pena detentiva da uno a cinque anni. La stessa Legge 69/2015 introduce anche due nuovi reati presupposto: artt. 2621 bis e 2621 ter "reato di false comunicazioni sociali commesso con fatti di lieve entità".

[10] L'art 25-*quater* è stato introdotto nel d.lgs. 231/2001 dall'art. 3 della legge 14 gennaio 2003, n. 7. Si tratta dei "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali*", nonché dei delitti, diversi da quelli sopra indicati, "*che siano comunque stati posti in essere in violazione di quanto previsto dall'articolo 2 della Convenzione internazionale per la repressione del finanziamento del terrorismo fatta a New York il 9 dicembre 1999*". Tale Convenzione, punisce chiunque, illegalmente e dolosamente, fornisce o raccoglie fondi sapendo che gli stessi saranno, anche parzialmente, utilizzati per compiere: (i) atti diretti a causare la morte - o gravi lesioni - di civili, quando l'azione sia finalizzata ad intimidire una popolazione, o coartare un governo o un'organizzazione internazionale; (ii) atti costituenti reato ai sensi delle convenzioni in materia di: sicurezza del volo e della navigazione, tutela del materiale nucleare, protezione di agenti diplomatici, repressione di attentati mediante uso di esplosivi. La categoria dei "*delitti aventi finalità di terrorismo o di eversione dell'ordine democratico, previsti dal codice penale e dalle leggi speciali" è* menzionata dal Legislatore in modo generico, senza indicare le norme specifiche la cui violazione comporterebbe l'applicazione del presente articolo. Si possono, in ogni caso, individuare quali principali reati presupposti l'art. 270-*bis* c.p. (*Associazioni con finalità di terrorismo anche internazionale o di eversione dell'ordine democratico*) il quale punisce chi promuove, costituisce organizza, dirige o finanzia associazioni che si propongono il compimento di atti violenti con finalità terroristiche od eversive, e l'art. 270-*ter* c.p. (*Assistenza agli associati*) il quale punisce chi dà rifugio o fornisce vitto, ospitalità mezzi di trasporto, strumenti di comunicazione a taluna delle persone che partecipano alle associazioni con finalità terroristiche od eversive.

[11] L'art 25-*quater1* è stato introdotto nel d.lgs. 231/2001 dall'art. 8 della legge 9 gennaio 2006, n. 7. Si tratta del reato di pratiche di mutilazione degli organi genitali femminili di cui all'art. 583-*bis* c.p.

i. delitti contro la personalità individuale, richiamati dall'art. 25-*quinquies* del Decreto[12];

j. delitti in materia di abusi di mercato, indicati all'art. 25-*sexies* del Decreto[13];

k. delitti di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme antinfortunistiche e sulla tutela dell'igiene e della salute sul lavoro, richiamati dall'art. 25-*septies* del Decreto[14];

l. reati transnazionali, indicati dall'art. 10 legge 16 marzo 2006, n. 146[15];

m. reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, richiamati dall'art. 25-*octies* del Decreto[16];

---

[12] L'art. 25-*quinquies* è stato introdotto nel d.lgs. 231/2001 dall'art. 5 della legge 11 agosto 2003, n. 228. Si tratta dei reati di riduzione o mantenimento in schiavitù o in servitù (art. 600 c.p.), tratta di persone (art. 601 c.p.), acquisto e alienazione di schiavi (art. 602 c.p.), reati connessi alla prostituzione minorile e allo sfruttamento della stessa (art. 600-*bis* c.p.), alla pornografia minorile e allo sfruttamento della stessa (art. 600-*ter* c.p.), detenzione di materiale pornografico prodotto mediante lo sfruttamento sessuale dei minori (art. 600-*quater* c.p.), iniziative turistiche volte allo sfruttamento della prostituzione minorile (art. 600-*quinquies* c.p.).

13 L'art. 25-*sexies* è stato introdotto nel d.lgs. 231/2001 dall'art. 9 della legge 18 aprile 2005 n. 62. Si tratta dei reati di abuso di informazioni privilegiate (art. 184, d.lgs. 58/1998) e di manipolazione del mercato (art. 185, d.lgs. 58/1998).

[14] L'art. 25-*septies* è stato introdotto nel d.lgs. 231/2001 dall'art. 300 del d.lgs. 9 aprile 2008, n. 81. Si tratta dei reati di omicidio colposo (art. 589, comma 2, c.p.) commesso con violazione delle norme sulla tutela della salute e sicurezza sul lavoro e delle lesioni personali gravi o gravissime (art. 590, comma 3, c.p.) commesse con violazione delle norme sulla tutela della salute e sicurezza sul lavoro.

[15] La legge 16 marzo 2006, n. 146, di ratifica ed esecuzione in Italia della Convenzione e dei Protocolli contro il crimine organizzato transnazionale, adottati dall'Assemblea generale delle Nazioni Unite il 15 novembre 2000 ed il 31 maggio 2001 (nota come *Convenzione di Palermo*), ha introdotto, mediante un'autonoma previsione contenuta nel suo art. 10, la responsabilità amministrativa degli enti in relazione a determinate ipotesi di c.d. "reato transnazionale".
La definizione di "reato transnazionale" è contenuta nell'art. 3 della medesima legge 146/2006, laddove si specifica che si considera tale "il reato punito con la pena della reclusione non inferiore nel massimo a quattro anni, qualora sia coinvolto un gruppo criminale organizzato", con l'ulteriore condizione che sussista almeno uno dei seguenti requisiti [art. 3, lett. a), b), c) e d)]:

(i) "sia commesso in più di uno Stato";
(ii) "sia commesso in uno Stato, ma una parte sostanziale della sua preparazione, pianificazione, direzione o controllo avvenga in un altro Stato";
(iii) "sia commesso in uno Stato, ma in esso sia implicato un gruppo criminale organizzato impegnato in attività criminali in più di uno Stato";
(iv) "sia commesso in uno Stato ma abbia effetti sostanziali in un altro Stato".

La ratifica della convenzione e dei suoi protocolli ha offerto l'occasione per includere numerosi nuovi reati al catalogo di quelli che fanno scattare la responsabilità degli enti.
L'art. 10 della L. 146/2006 dispone – in via di richiamo – nell'ultimo comma che "agli illeciti amministrativi previsti dal presente articolo si applicano le disposizioni di cui al decreto legislativo 8 giugno 2001, n. 231".
I reati transnazionali richiamati dall'art. 10 della L. 146/2006 sono i reati di associazione per delinquere (art. 416 c.p.), associazione di tipo mafioso anche straniera (art. 416-*bis* c.p.), induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria (art. 377-*bis* c.p.), favoreggiamento personale (art. 378 c.p.), associazione per delinquere finalizzata al contrabbando di tabacchi lavorati esteri (art. 291-*quater* D.P.R. 23 gennaio 1973, n. 43), associazione finalizzata al traffico illecito di sostanze stupefacenti o psicotrope (art. 74 D.P.R. 9 ottobre 1990, n. 309), reati concernenti il traffico di migranti (art. 12 d.lgs. 25 luglio 1998, n. 286).

[16] L'art. 25-*octies* è stato introdotto nel d.lgs. 231/2001 dall'art. 63, comma 3, del d.lgs. 21 novembre 2007, n. 231. Si tratta dei reati di ricettazione (art. 648 c.p.), riciclaggio (art. 648-*bis* c.p.) e impiego di denaro, beni o utilità di provenienza illecita (art. 648-*ter* c.p.). La Legge 15 dicembre 2014, n. 186 (G.U. n. 292 del 17 dicembre 2014) – recante "Disposizioni in materia di emersione e rientro di capitali detenuti all'estero nonché per il potenziamento della lotta all'evasione fiscale. Disposizioni in materia di autoriciclaggio" – ha introdotto nel codice penale il nuovo reato di

n. delitti in materia di violazione del diritto d'autore, richiamati dall'art. 25-*novies* del Decreto[17];

o. reato di induzione a non rendere dichiarazioni o a rendere dichiarazioni mendaci all'autorità giudiziaria, richiamato dall'art. 25-*decies* del Decreto[18];

p. reati ambientali, richiamati dall'art. 25-*undecies*[19];

q. Impiego di cittadini di paesi terzi il cui soggiorno è irregolare, richiamato nell'art. 25 -

autoriciclaggio. La stessa legge interviene, altresì, in materia di responsabilità amministrativa degli enti, prevedendo l´inserimento del nuovo reato di autoriciclaggio tra quelli richiamati dall´art. 25-octies del D.Lgs. 231/2001.

[17] L'art. 25-*novies* è stato introdotto nel d.lgs. 231/2001 dall'art. 15 della L. 99/2009. Si tratta dei reati previsti dagli artt. 171, 171-*bis*, 171-*ter*, 171-*septies*, 171-*octies*, Legge 22 aprile 1941, n. 633 (Protezione del diritto d'autore e di altri diritti connessi al suo esercizio).

[18] Per un difetto di coordinamento con la Legge "Sviluppo Energia" (L.99/2009) il presente articolo è stato inizialmente inserito nel d.lgs. 231/01 con identica numerazione rispetto all'articolo " i delitti in materia di violazione del diritto d'autore". Il d.lgs. 121/2011 ha fornito al legislatore l'occasione per rimediare all'errore compiuto, rinumerando l'articolo 25-novies relativo all'art. 377–*bis* c.p. come 25–*decies.*

[19] L'art. 25-*undecies* è stato introdotto nel d.lgs. 231/2001 dall'art. 2, comma 3, del d.lgs. 7 luglio 2011, n. 121, recante "Attuazione della Direttiva 2008/99/CE sulla tutela penale dell'ambiente, nonché della direttiva 2009/123/CE che modifica la direttiva 2005/35/CE relativa all'inquinamento provocato dalle navi e all'introduzione di sanzioni per violazioni". In particolare, la Direttiva 2008/99/CE (pubblicata sulla G.U.C.E. del 6 dicembre 2008) ha disposto un notevole ampliamento delle fattispecie di reati ambientali sanzionabili a norma del d.lgs. 231/2001. In particolare, ha chiarito che gli Stati Membri dovranno provvedere affinché le persone giuridiche possano essere dichiarate responsabili di reati tra i quali, a titolo esemplificativo:

- scarico, emissione o immissione di sostanze/radiazioni nell'aria, nel suolo o nelle acque che provochino decesso, lesioni gravi alle persone o danni rilevanti alla qualità dell'aria, del suolo, delle acque o alla flora e fauna;
- raccolta, trasporto, recupero o smaltimento dei rifiuti che provochi (o possa provocare) il decesso o lesioni gravi alle persone o danni rilevanti alla qualità dell'aria, del suolo, delle acque o alla flora e fauna;
- esercizio di impianti in cui siano svolte attività pericolose o nelle quali siano depositate o utilizzate sostanze o preparazioni pericolose che provochino (possano provocare) danni a persone o all'ambiente;
- produzione, lavorazione, trattamento, uso, conservazione, deposito, importazione, esportazione e smaltimento di materiali nucleari o di altre sostanze radioattive pericolose che provochino (possano provocare) danni a persone o all'ambiente.

  La legge 68/2015 riguardante "Disposizioni in materia di delitti contro l'ambiente" inserisce nel Codice Penale un nuovo Titolo, VI-bis, dedicato ai delitti contro l'ambiente all'interno del quale sono stati previsti cinque nuovi reati (452-bis c.p. Inquinamento ambientale;452-quater c.p. Disastro ambientale; 452-sexies c.p. Traffico e abbandono di materiale ad alta radioattività; 452-septies c.p. Impedimento del controllo; 452-terdecies c.p. Omessa bonifica. La legge 68/2015 modifica inoltre l'art 25-undecies del D.Lgs. 231/01, aggiungendo tra i reati presupposto: il delitto di inquinamento ambientale (art. 425-bis c.p.) prevedendo per tale violazione la sanzione pecuniaria da duecentocinquanta a seicento quote; il delitto di disastro ambientale (art. 452-quater c.p.) prevedendo per tale violazione la sanzione pecuniaria da quattrocento a ottocento quote; i delitti colposi contro l'ambiente (art.452-quinquies c.p.), prevedendo per tale violazione la sanzione pecuniaria da duecento a cinquecento quote; per i delitti associativi aggravati ai sensi dell'articolo 452-octies, la sanzione pecuniaria da trecento a mille quote; il delitto di traffico e abbandono di materiale ad alta radioattività (art. 452-sexies c.p.) prevedendo per tale violazione la sanzione pecuniaria da duecentocinquanta a seicento quote. La legge prevede inoltre che per i reati di inquinamento ambientale e di disastro ambientale si applichino, oltre alle sanzioni pecuniarie ivi previste, le sanzioni interdittive previste dall'articolo 9 del D.Lgs. 231/01, stabilendo una durata massima di 1 anno in relazione al delitto di inquinamento. La legge 68/2015 non richiama nei confronti degli enti la possibilità del ravvedimento operoso prevista all'art. 452 decies c.p. pertanto sarà applicabile l'attenuante dell'art. 12 del D.Lgs.231/01 che prevede che la sanzione pecuniaria venga ridotta da un terzo alla metà se prima dell'apertura del dibattimento l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è efficacemente adoperato in tal senso.

duodecies[20];

r. delitti in materia di discriminazione razziale e xenofobia richiamati dall'art. 25 - *terdecies*[21];

s. frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati, richiamati dall'art. 25 - *quaterdecies* [22];

t. i reati cosiddetti tributari, richiamati dall'art. 25 - quinquiesdecies[23];

u. reati di contrabbando, richiamati dall'art. 25 - sexiesdecies [24]

Lo scenario appena descritto è peraltro destinato ad evolversi e comporterà l'aggiornamento tempestivo del Modello in caso inserimento di nuovi reati o di modifica di quelli esistenti nell'ambito del Decreto.

---

[20] L'art. 25-*duodecies* è stato introdotto nel d.lgs. 231/2001 dall'art. 2, comma 1, successivamente modificato dalla L. 167/2017 che prevede il reato di ingresso illegale di stranieri in Italia o altro Stato.

[21] L'art. 25-terdecies è stato introdotto nel d.lgs. n. 231/2001 dall'art. 5, comma 2, della legge 20 novembre 2017, n. 167.

[22] L'art. 25-*quaterdecies* è stato introdotto nel d.lgs. n. 231/2001 dall'art. 5 della Legge 3 maggio 2019 n.39.

[23] Il secondo comma dell'art. 39 del decreto legge 26 ottobre 2019 n.124 recante "*Disposizioni urgenti in materia fiscale e per esigenze indifferibili*" (il "Decreto Fiscale"), convertito con modifiche dalla L. n. 157/201, ha esteso la responsabilità amministrativa degli enti ai reati tributari, introducendo nel d.lgs. 231/01 l'art. 25- quinquiesdecies. In particolare si tratta dei delitti di cui agli articoli 2, 3, 8, 10 ed 11 del d.lgs. 74 del 10 marzo 2000: (i) dichiarazione fraudolenta mediante uso di fatture o altri documenti per operazioni inesistenti (art. 2, comma 1 e 2 bis del d.lgs 74/2000); (ii) dichiarazione fraudolenta mediante altri artifici (art. 3 del d.lgs 74/2000); (iii) emissione di fatture o altri documenti per operazioni inesistenti (art. 8 del d.lgs 74/2000); (iv) occultamento o distruzione di documenti contabili (art. 10 del d.lgs 74/2000) e (v) sottrazione fraudolenta al pagamento di imposte (art. 11 del d.lgs 74/2000).
Con il D. lgs del 14 luglio 2020 n. 75, recante l'attuazione della direttiva UE 2017/1371 relativa alla lotta contro la frode che lede gli interessi finanziari dell'UE mediante il diritto penale, il legislatore ha modificato l'articolo 25 – *quinquiesdecies* del D.lgs 231/2001 inserendo dopo il comma 1 il seguente: «1 -*bis*. *In relazione alla commissione dei delitti previsti dal decreto legislativo 10 marzo 2000, n. 74, se commessi nell'ambito di sistemi fraudolenti transfrontalieri e al fine di evadere l'imposta sul valore aggiunto per un importo complessivo non inferiore a dieci milioni di euro, si applicano all'ente le seguenti sanzioni pecuniarie:*
a) per il delitto di dichiarazione infedele previsto dall'articolo 4, la sanzione pecuniaria fino a trecento quote;
b) per il delitto di omessa dichiarazione previsto dall'articolo 5, la sanzione pecuniaria fino a quattrocento quote;
c) per il delitto di indebita compensazione previsto dall'articolo 10 -quater , la sanzione pecuniaria fino a quattrocento quote.»
Inoltre al comma 2, le parole «al comma 1» sono sostituite dalle seguenti: «ai commi 1 e 1 -*bis* »; ed infine al comma 3, le parole «commi 1 e 2» sono sostituite dalle seguenti: «commi 1, 1 -*bis* e 2»

[24] Con il D. lgs del 14 luglio 2020 n. 75, recante l'attuazione della direttiva UE 2017/1371, relativa alla lotta contro la frode che lede gli interessi finanziari dell'UE mediante il diritto penale, il legislatore con l'art. 5 interviene sul d. lgs. 231/2001, ampliando il novero dei reati-presupposto della responsabilità dell'ente introducendo l'art. 25 -*sexiesdecies (Contrabbando)*
"1. In relazione alla commissione dei reati previsti dal decreto del Presidente della Repubblica 23 gennaio 1973, n. 43, si applica all'ente la sanzione pecuniaria fino a duecento quote.
2. Quando i diritti di confine dovuti superano centomila euro si applica all'ente la sanzione pecuniaria fino a quattrocento quote.
3. Nei casi previsti dai commi 1 e 2 si applicano all'ente le sanzioni interdittive previste dall'articolo 9, comma 2, lettere c) , d) ed e) ."

1.3 PRESUPPOSTI PER L'IMPUTAZIONE ALL'ENTE DELLA RESPONSABILITÀ AMMINISTRATIVA

Per accertare la responsabilità dell'ente, l'art. 5 del d.gs. 231/01 indica criteri di imputazione oggettivi e soggettivi.

1.3.a) Criteri di imputazione oggettivi e soggettivi

Per quanto concerne il **criterio oggettivo** di imputazione, il Decreto stabilisce che l'ente è responsabile per i reati previsti agli artt. 24 e ss., **commessi nel suo interesse o a suo vantaggio** da persone appartenenti alla sua struttura organizzativa.

L'**interesse** è identificato nel fine della condotta delittuosa della persona fisica e per questo viene valutato ex ante, al momento dell'azione; infatti l'attuazione dell'interesse può verificarsi, ma anche rimanere solo potenziale.

Il **vantaggio**, invece, è identificato da un profitto materiale ottenuto grazie alla commissione del reato anche indipendentemente dall'interesse del soggetto agente; infatti il vantaggio è sempre associato a beni materiali riconducibili al patrimonio.

Per quanto concerne invece il **criterio soggettivo** di imputazione, il Decreto stabilisce che i reati-presupposto devono essere stati commessi dalle persone in posizione di vertice o da quelle sottoposte alla direzione o vigilanza delle prime. In particolare, l'articolo 5 del Decreto dispone che l'ente sia ritenuto responsabile se il reato viene posto in essere:

a) da persone che rivestono *funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unità organizzativa dotata di una sua autonomia finanziaria e funzionale nonché da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso* (i c.d. soggetti "in posizione apicale" o "**apicali**"; art. 5, comma 1, lett. a), del Decreto);

b) da persone *sottoposte alla direzione o alla vigilanza di uno dei soggetti appena menzionati* (i c.d. soggetti **sottoposti** all'altrui direzione; art. 5, comma 1, lett. b), del Decreto).

Si noti come nel caso di cui al punto a), il soggetto debba esercitare un vero e proprio dominio sull'ente. Resta pertanto escluso dall'orbita della predetta disposizione l'esercizio di una funzione di controllo assimilabile, ad esempio, a quella svolta dai sindaci.

Si ritiene, invece, che nell'ambito degli apicali rientrino, oltre ai Dirigenti, anche i Responsabili di Area non dirigenti in quanto, nel dare concreta esecuzione alle attività di direzione della Società, svolgono un'attività assimilabile, in termini di responsabilità, a quella dei Responsabili di Area con qualifica dirigenziale.

1.3.b) Reato-presupposto commesso da soggetti apicali

Nell'ipotesi di un reato-presupposto commesso da *soggetti apicali*, l'ente non risponderà se prova che:

- → l'organo dirigente ha adottato ed efficacemente attuato, prima della commissione del fatto, un Modello di Organizzazione, Gestione e Controllo idoneo a prevenire reati della specie di quello verificatosi;
- → sia stato affidato a un organismo dell'ente dotato di autonomi poteri di iniziativa e di controllo (OdV) il compito di vigilare sul funzionamento e l'osservanza del Modello e di curarne l'aggiornamento;
- → non vi sia stata omessa o insufficiente vigilanza da parte dell'organismo di controllo in ordine al Modello;
- → i soggetti abbiano commesso il reato eludendo fraudolentemente il Modello, ovvero a proprio ed esclusivo interesse (o vantaggio).

1.3.c) Reato-presupposto commesso da soggetti sottoposti

Nel caso in cui il reato sia stato commesso da *soggetti sottoposti* alla direzione o alla vigilanza del personale apicale, l'ente sarà ritenuto responsabile del reato solamente in ipotesi di carenza colpevole negli obblighi di direzione e vigilanza: dunque, la responsabilità dell'ente si configura solo se la commissione del reato è stata resa possibile dall'inosservanza degli obblighi di direzione e di vigilanza da parte di soggetti con poteri di gestione.

Inoltre l'ente non risponderà se prova che prima della commissione del reato sono stati adottati ed attuati i Modelli di organizzazione e di gestione idonei a prevenire reati della specie di quello verificatosi. Affinché il Modello di Organizzazione, Gestione e Controllo abbia valore esimente è dunque determinante la sua formale adozione precedente al fatto-reato e l'efficace attuazione da parte dell'ente stesso.

* * *

L'adozione dei "Modelli di organizzazione e gestione" adempie, pertanto, ad una funzione meramente preventiva. Piuttosto che sancire un generico dovere di vigilanza e di controllo della società si è preferito utilizzare il sistema dei *compliance programs* da tempo funzionante negli Stati Uniti. Alla società viene in pratica richiesta l'adozione di modelli comportamentali specificatamente calibrati sul rischio-reato, e cioè volti ad impedire, attraverso la fissazione di regole di condotta, la commissione di determinati atti.

Requisito indispensabile perché dall'adozione del modello derivi l'esenzione da responsabilità dell'ente è che esso venga anche efficacemente attuato: l'effettività rappresenta, dunque, un punto qualificante ed irrinunciabile del nuovo sistema di responsabilità.

L'adozione di un tale strumento, ad opera del Consiglio di Amministrazione (o dell'Amministratore Unico, se del caso) costituisce un onere per la società, il cui rispetto permette di beneficiare delle esenzioni da responsabilità e di altri benefici in termini di riduzione delle sanzioni; non è un obbligo di cui si sanziona l'inadempienza.

1.4 LE SANZIONI PREVISTE DAL DECRETO

Al verificarsi delle condotte sanzionate dal Decreto sono previste a carico dell'ente:

a) **sanzioni pecuniarie**: da un minimo di circa 25 mila Euro fino a un massimo di circa un milione e mezzo di Euro (e sequestro conservativo in sede cautelare)[25], la cui valutazione è lasciata alla discrezionalità del giudice secondo la gravità del fatto, alla responsabilità dell'ente e alla eventuale attività posta in essere per riparare le conseguenze dell'atto illecito e per prevenirne altri;

b) **sanzioni interdittive**;

oltre a

c) **confisca** (e sequestro preventivo in sede cautelare);

d) **pubblicazione della sentenza** (in caso di applicazione di una sanzione interdittiva).

Le sanzioni interdittive hanno una durata non inferiore a tre mesi e non superiore a due anni (ai sensi dell'art. 14, comma 1, del Decreto, esse "*hanno ad oggetto la specifica attività alla quale si riferisce l'illecito dell'ente*"); possono consistere in:

b.1 interdizione dall'esercizio dell'attività;

b.2 sospensione o revoca delle autorizzazioni, licenze o concessioni funzionali alla commissione dell'illecito;

b.3 divieto di contrattare con la Pubblica Amministrazione, salvo che per ottenere le prestazioni di un pubblico servizio;

b.4 esclusione da agevolazioni, finanziamenti, contributi o sussidi e l'eventuale revoca di quelli concessi;

b.5 divieto di pubblicizzare beni o servizi.

Le sanzioni interdittive si applicano in relazione ai soli reati per i quali siano espressamente previste[26], in presenza di una delle seguenti condizioni: (i) l'ente abbia tratto dalla consumazione

[25] Con riferimento ai reati di c.d. *Market Abuse* (abuso di informazioni privilegiate e manipolazione del mercato, di cui agli artt. 184 e 185 d.lgs. 58/1998: *cfr.* sopra, § 1.2), l'art. 25-*sexies* d.lgs. 231/2001 prevede, per il caso in cui in seguito alla commissione di tali reati il prodotto o il profitto conseguito dall'ente sia di rilevante entità, la possibilità di aumento della sanzione pecuniaria fino a dieci volte tale prodotto o profitto.

[26] Si tratta di: reati contro la pubblica amministrazione di cui agli artt. 24 e 25 d.lgs. 231/2001; delitti informatici e trattamento illecito di dati di cui all'art. 24-*bis* d.lgs. 231/2001; delitti di criminalità organizzata di cui all'art. 24-*ter* d.lgs. 231/2001; taluni reati contro la fede pubblica quali la falsità in monete di cui all'art. 25-*bis* d.lgs. 231/2001; delitti contro l'industria e il commercio di cui all'art. 25-*bis1* d.lgs. 231/2001; delitto di corruzione tra privati di cui all'art. 25-*ter lett.s-bis)* d.lgs. 231/2001; delitti in materia di terrorismo e di eversione dell'ordine democratico di cui all'art. 25-*quater* d.lgs. 231/2001; pratiche di mutilazione degli organi genitali femminili, di cui all'art. 25-*quater1* d.lgs. 231/2001; delitti contro la personalità individuale, di cui all'art. 25-*quinquies* d.lgs. 231/2001; delitti di omicidio colposo e lesioni colpose gravi o gravissime commessi con violazione delle norme sulla tutela della salute e sicurezza sul lavoro, di cui all'art. 25-*septies* d.lgs. 231/2001; reati di ricettazione, riciclaggio e impiego di denaro, beni o utilità di provenienza illecita, di cui all'art. 25-*octies* d.lgs. 231/2001; delitti in materia di violazione del diritto d'autore di cui all'art. 25-*novies* d.lgs. 231/2001; taluni reati contro l'ambiente di cui all'art. 25-*undecies*; impiego di cittadini di paesi terzi il cui soggiorno è irregolare, di cui all'art. *25- duodecies* d.lgs. 231/2001; delitti di razzismo e xenofobia, di cui all'art. 25-*terdecies* d.lgs 231/01; frode in competizioni sportive, esercizio abusivo di gioco o scommessa e giochi d'azzardo esercitati a mezzo di apparecchi

del reato un profitto di rilevante entità e il reato sia stato commesso da soggetti in posizione apicale ovvero da soggetti sottoposti all'altrui direzione quando, in tale ultimo caso, la commissione del reato sia stata determinata o agevolata da gravi carenze organizzative; (ii) in caso di reiterazione degli illeciti.

Sono previste sanzioni interdittive più severe per i reati contro la P.A. (artt. 317, 319, 319-ter, 319-quater, 322, commi 2 e 4, c.p.), operando anche una distinzione tra reato commesso dal soggetto apicale e reato commesso dal soggetto "sottoposto": nel primo caso, la durata delle interdittive sarà compresa tra 4 e 7 anni; nel secondo caso, tra 2 e 4 anni.

Ai sensi dell'art. 45 del Decreto, le sanzioni interdittive sono applicabili anche in via cautelare, su richiesta del pubblico ministero. Le "misure cautelari" saranno quindi disposte in presenza di gravi indizi di responsabilità, da cui, inoltre, risulti attuale e concreto il pericolo che siano reiterate medesime condotte criminose.

Per completezza, deve altresì evidenziarsi che il Modello, oltre a essere un utile strumento di prevenzione del rischio-reato, può assicurare anche una funzione di natura riparatoria**,** nei casi in cui la sua adozione o il suo adeguamento si realizzi *post delictum* purché ricorrano le condizioni di cui agli artt. 12 e 17 del Decreto[27], con il beneficio di poter ottenere una considerevole riduzione della sanzione pecuniaria nonché l'inapplicabilità delle sanzioni interdittive.

1.5 REQUISITI DEL MODELLO - LE LINEE GUIDA EMANATE DALL'ASSOCIAZIONE DI CATEGORIA (CONFINDUSTRIA) E CIRCOLARE N. 83607/2012 DELLA GUARDIA DI FINANZA

vietati, di cui all'art. 25-*quaterdecies* d.lgs 231/01; reati tributari di cui all'art. 25- quinquiesdecies; reati di contrabbando di cui all'art. 25 -*sexiesdecies*

[27] Art. 12. Casi di riduzione della sanzione pecuniaria
1. La sanzione pecuniaria è ridotta della metà e non può comunque essere superiore a lire duecento milioni se:
a) l'autore del reato ha commesso il fatto nel prevalente interesse proprio o di terzi e l'ente non ne ha ricavato vantaggio o ne ha ricavato un vantaggio minimo;
b) il danno patrimoniale cagionato è di particolare tenuità.
2. La sanzione è ridotta da un terzo alla metà se, prima della dichiarazione di apertura del dibattimento di primo grado:
a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
b) è stato adottato e reso operativo un modello organizzativo idoneo a prevenire reati della specie di quello verificatosi.
3. Nel caso in cui concorrono entrambe le condizioni previste dalle lettere del precedente comma, la sanzione è ridotta dalla metà ai due terzi.
4. In ogni caso, la sanzione pecuniaria non può essere inferiore a lire venti milioni.
Art. 17. Riparazione delle conseguenze del reato
1. Ferma l'applicazione delle sanzioni pecuniarie, le sanzioni interdittive non si applicano quando, prima della dichiarazione di apertura del dibattimento di primo grado, concorrono le seguenti condizioni:
a) l'ente ha risarcito integralmente il danno e ha eliminato le conseguenze dannose o pericolose del reato ovvero si è comunque efficacemente adoperato in tal senso;
b) l'ente ha 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;
c) l'ente ha messo a disposizione il profitto conseguito ai fini della confisca.

"*I modelli di organizzazione e di gestione possono essere adottati, garantendo le esigenze di cui al comma 2, sulla base di codici di comportamento redatti dalle associazioni rappresentative degli enti, comunicati al Ministero della Giustizia che, di concerto con i Ministeri competenti, può formulare, entro trenta giorni, osservazioni sulla idoneità dei modelli a prevenire i reati*" (art. 6, comma 3).

Confindustria ha adottato le "*Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001*"(aggiornate da Confindustria e approvate dal Ministero Giustizia il 21 luglio 2014). Successivamente, nel mese di febbraio 2019, il Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili congiuntamente ad ABI, al Consiglio Nazionale Forense e a Confindustria, ha elaborato il documento denominato "*Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza, prospettive di revisione del d.lgs. 8 giugno 2001 n. 231*" che, in ragione delle esperienze dei diversi soggetti firmatari, indica i principi per la redazione dei Modelli organizzativi ex D.Lgs. 231/2001 e per lo svolgimento delle attività dell'Organismo di Vigilanza, evidenziando, al contempo, alcune proposte di modifica alla normativa vigente.

Le caratteristiche essenziali per la costruzione di un Modello di organizzazione, gestione e controllo ivi indicate sono:

a. l'identificazione dei rischi, ossia l'analisi delle strutture aziendali al fine di evidenziare da dove (in quale divisione/area e/o settore di attività) e secondo quali modalità si possano verificare le ipotesi criminose previste dal d.lgs. 231/2001;

b. la progettazione del sistema di controllo (c.d. *protocolli*), ossia la valutazione del sistema di controllo esistente e l'eventuale adeguamento, al fine di contrastare efficacemente i rischi precedentemente individuati. Le componenti di un sistema di controllo preventivo sui rischi di reato sono così individuate:

   b.1 adozione di un codice etico con riferimento ai reati considerati;

   b.2 adozione di un sistema organizzativo sufficientemente formalizzato e chiaro soprattutto per quanto concerne l'attribuzione di responsabilità;

   b.3 adozione di procedure manuali e informatiche;

   b.4 adozione di un sistema di poteri autorizzativi e di firma;

   b.5 adozione di un sistema di controllo di gestione;

   b.6 adozione di un sistema di comunicazione e formazione del personale.

   Le componenti sopra evidenziate devono ispirarsi ai seguenti principi:

   (i) ogni operazione, transazione, azione deve essere verificabile, documentata, coerente e congrua;

   (ii) nessuno può gestire in autonomia un intero processo;

   (iii) il sistema di controllo deve documentare lo svolgimento dei controlli;

c. la costituzione dell'Organismo di Vigilanza[28], ossia dell'organo al quale affidare il compito di vigilare sul funzionamento, sull'efficacia e l'osservanza del Modello di Organizzazione, Gestione e Controllo, nonché di curarne l'aggiornamento;

d. la previsione di un autonomo sistema disciplinare o di meccanismi sanzionatori per le violazioni delle norme del codice etico e del Modello di Organizzazione, Gestione e Controllo.

[28] L'art. 14, comma 12, L. 12 novembre 2011 n. 183, modificato dall'art. 16, comma 2, d.l. 22 dicembre 2011 n. 212, successivamente soppresso dalla *legge di conversione 17 febbraio 2012, n. 10*, ha previsto l'inserimento del comma 4bis nell'art. 6 del d.lgs 231/01, il quale stabilisce che "*Nelle società di capitali il collegio sindacale, il consiglio di sorveglianza e il comitato per il controllo della gestione, possono svolgere la funzione dell'organismo di vigilanza di cui al comma 1, lett. b)*".

CAPITOLO 2
LA STRUTTURA ORGANIZZATIVA ED AZIENDALE DI CONSIP SpA

2.1 LE ATTIVITÀ

Consip è una società per azioni totalmente partecipata dal Ministero dell'Economia e delle Finanze (nel seguito in breve "MEF"), che opera secondo gli indirizzi strategici del Ministero stesso e lavora al servizio esclusivo della Pubblica Amministrazione; è qualificabile come società *in house* al Ministero, che esercita il controllo analogo ai sensi dell'art. 11[29] dello statuto sociale.

La Società svolge attività in favore delle Amministrazioni Pubbliche nei seguenti ambiti:

- Area Programma Acquisti - realizzazione del Programma di razionalizzazione della spesa pubblica per beni e servizi che Consip gestisce per conto del MEF e che prevede il consolidamento e lo sviluppo degli strumenti di acquisto e di negoziazione (tra cui gli

[29] Articolo 11
11.1 La gestione dell'impresa spetta esclusivamente all'Amministratore Unico o agli Amministratori, i quali compiono le operazioni necessarie per l'attuazione dell'oggetto sociale in osservanza delle direttive di cui al comma successivo.
11.2 Gli Amministratori si conformano alle direttive pluriennali impartite dal Dipartimento del Tesoro in ordine alle strategie, al piano delle attività, all'organizzazione, alle politiche economiche, finanziarie e di sviluppo. Tali direttive sono emanate dal Dipartimento del Tesoro, sentite le altre Amministrazioni affidanti, e, per gli aspetti afferenti le attività svolte da Consip in favore di Sogei, ai sensi dell'articolo 4.1 lett. a), sentiti il Dipartimento delle Finanze e il Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi. Le direttive sono emanate entro il 30 novembre di ogni anno e preventivamente comunicate all'azionista ai fini della verifica dei profili economici e finanziari.
11.3 Entro il 31 dicembre, in attuazione delle direttive di cui al comma precedente, gli Amministratori comunicano al Dipartimento del Tesoro un piano generale annuale concernente le attività, gli investimenti e l'organizzazione. Decorsi trenta giorni dalla trasmissione al Dipartimento, il piano generale annuale si intende approvato.
11.4 Per l'affidamento diretto delle attività di cui all'articolo 4.1 lett. a) e b), la Società sottoscrive con le Pubbliche Amministrazioni affidanti di riferimento appositi Disciplinari, previa informativa (i) al Dipartimento del Tesoro, e (ii) all'azionista unico, ai fini della verifica del mantenimento dell'equilibrio economico-finanziario.
11.5 Al fine di garantire l'effettività del "controllo analogo", le funzioni di orientamento, supervisione, monitoraggio e verifica relative alle attività operative di cui ai Disciplinari stipulati ai sensi del comma precedente sono rimesse alle Amministrazioni affidanti. I medesimi Disciplinari individueranno, altresì: le risorse umane, finanziarie e strumentali da impiegare; i meccanismi di copertura delle spese di funzionamento e degli oneri di gestione; la tempistica degli adempimenti e i criteri di rendicontazione dei fatti economici mediante contabilità separate.
11.6 Le Convenzioni di cui all'articolo 4.1 lett. c), d) ed e) sono sottoposte al vaglio preventivo del Dipartimento del Tesoro ai fini della verifica della permanenza dei requisiti del rapporto in house e della coerenza con le direttive impartite, nonché all'azionista per la verifica dei profili economici e finanziari. Le convenzioni individuano i criteri di rendicontazione dei fatti economici mediante contabilità separata.
11.7 Gli Amministratori informano trimestralmente, attraverso rapporti sulla gestione e amministrazione, il Dipartimento del Tesoro e l'azionista che verificano, rispettivamente, la rispondenza dell'azione sociale alle direttive impartite e agli indirizzi annuali approvati, e il mantenimento dell'equilibrio economico-finanziario.
11.8 Il Dipartimento del Tesoro ha diritto di avere dagli Amministratori notizie e informazioni sulla gestione e amministrazione della Società.
11.9 Sono inoltre attribuite al Consiglio di Amministrazione, previa informativa al socio, le seguenti competenze:
a) l'istituzione e la soppressione di sedi secondarie;
b) l'indicazione di quali Amministratori abbiano la rappresentanza della società;
c) l'adeguamento dello statuto sociale a disposizioni normative obbligatorie, che non comportino valutazioni discrezionali in merito alle modalità di recepimento delle stesse;
d) il trasferimento della sede sociale all'interno del territorio nazionale.
11.10 L'assemblea straordinaria può attribuire agli Amministratori la facoltà di emettere in una o più volte obbligazioni convertibili, fino ad un ammontare determinato e per il periodo massimo di cinque anni dalla data di adozione del presente statuto. In tal caso la delega comprende anche quella relativa al corrispondente aumento del capitale sociale.

strumenti di *e-procurement*) messi a disposizione delle P.A., quali Convenzioni, Mercato elettronico della PA (MePA), Accordi Quadro, Sistema Dinamico di Acquisizione, gare su delega e in modalità ASP (*Application Service Provider*), progetti specifici per singole Amministrazioni;

- Area Procurement verticale - attività di centrale di committenza che Consip svolge per tutte le Amministrazioni (es. le gare a supporto dell'attuazione dell'Agenda Digitale), ovvero per singole Amministrazioni sulla base di apposite convenzioni, ai sensi di quanto disposto dall'articolo 29 del D.L. 201/2011 e s.m.i.);
- Area Affidamenti di legge - iniziative che coinvolgono Consip nel supporto a società, enti pubblici e Amministrazioni, sulla base di previsioni di legge e atti amministrativi del Ministero dell'Economia e delle Finanze in tema di revisione della spesa, razionalizzazione dei processi e innovazione nella PA; tra queste si evidenzia, a mero titolo esemplificativo, lo svolgimento di attività di supporto alla tenuta del Registro dei Revisori Legali e del Registro del Tirocinio, nonché di supporto nella gestione, valorizzazione e privatizzazione delle partecipazioni azionarie detenute dalla P.A. (ex SICOT).

2.2 CORPORATE GOVERNANCE

La Società ha adottato un modello classico di *corporate governance,* articolato come segue:

Assemblea degli Azionisti	
	organo attraverso cui l'Azionista unico (Ministero dell'economia e delle finanze) esprime la volontà sociale, che viene poi attuata dall'organo amministrativo – è competente a deliberare in sede ordinaria e straordinaria sulle materie riservate dalla legge e dallo statuto
Consiglio di Amministrazione	
	organo cui è demandata l'amministrazione ordinaria e straordinaria della Società, con facoltà di compiere tutti gli atti opportuni per l'attuazione ed il raggiungimento degli scopi sociali, ad esclusione degli atti riservati all'Assemblea - ai sensi dell'art. 12.1 dello statuto, il C.d.A. è attualmente composto da tre membri eletti dall'Assemblea, che devono possedere specifici requisiti di onorabilità, professionalità e competenza per l'assunzione della carica, in ossequio allo statuto ed alle norme vigenti in materia
Presidente	
	ha la rappresentanza della Società ed esercita i compiti definiti dal codice civile in tema di gestione delle riunioni consiliari/assembleari – ai sensi dell'art. 15.1 dello statuto può esercitare le deleghe operative conferite dal C.d.A. sulla base delle indicazioni in tal senso impartite dall'Assemblea

Amministratore Delegato	organo cui è affidata la gestione della Società in base ai poteri attribuitigli dal Consiglio di Amministrazione – ai sensi dell'art. 15.5 dello statuto, riferisce al C.d.A. e al Collegio Sindacale con cadenza trimestrale sull'andamento della gestione, sulla prevedibile evoluzione, nonché sulle operazioni di maggior rilievo effettuate dalla Società
Collegio Sindacale	organo cui spetta il compito di vigilare, ai sensi dell'art. 21 dello statuto su: a) osservanza della legge e dello statuto; b) rispetto dei principi di corretta amministrazione; c) adeguatezza dell'assetto amministrativo, organizzativo e contabile della Società e sul suo concreto funzionamento - ai sensi dell'art. 6 del D.M. 24/02/2000 il CS relaziona il Mef sull'andamento della gestione, sull'economicità e l'efficacia delle operazioni di cui al Programma di razionalizzazione degli acquisti di beni e servizi per le PA

2.3 ORGANIZZAZIONE INTERNA E STRUTTURA ORGANIZZATIVA

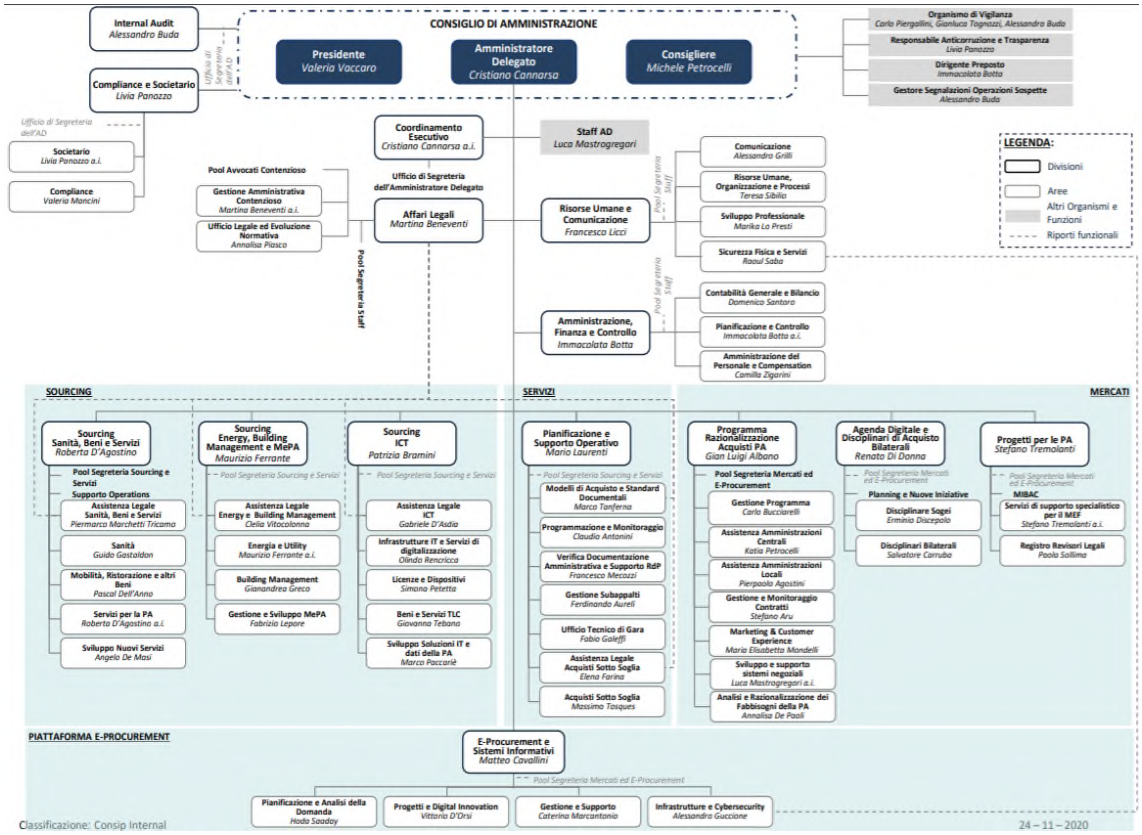
Dal punto di vista organizzativo, Consip si avvale di una struttura imperniata sul principio della separazione delle funzioni, che prevede la suddivisione in:

- Divisioni di staff
  al servizio della struttura complessivamente intesa
  - ✓ Divisione Amministrazione, Finanza e Controllo
  - ✓ Divisione Affari Legali
  - ✓ Divisione Risorse Umane e Comunicazione
  - ✓ Divisione Coordinamento Esecutivo
- Mercati
  gestiscono i Disciplinari/Convenzioni di business e gli accordi di collaborazione con gli enti, identificando gli ambiti di intervento e le azioni volte al raggiungimento degli obiettivi
  - ✓ Divisione Programma Razionalizzazione Acquisti P.A.
  - ✓ Divisione Progetti per la P.A.
  - ✓ Divisione Agenda Digitale e Disciplinari di Acquisto Bilaterali
- Sourcing
  garantiscono l'attuazione dei programmi e dei piani definiti nell'ambito dei singoli Disciplinari/Convenzioni e del Piano Acquisti Consip, per le iniziative di acquisto inerenti le merceologie di competenza
  - ✓ Divisione Sourcing Sanità, Beni e Servizi
  - ✓ Divisione Sourcing Energy, Building Management e MePA
  - ✓ Divisione Sourcing ICT
- Divisione E-Procurement e Sistemi informativi

assicura la progettazione e lo sviluppo dei sistemi informativi interni e della piattaforma di e-procurement garantendone la gestione e l'evoluzione, con particolare riguardo allei attività di prevenzione, rilevazione e risoluzione delle minacce alla sicurezza logica e fisica.

- Divisione Pianificazione e Supporto Operativo
  supporta le Divisioni Sourcing e Mercati nella progettazione e realizzazione delle iniziative di acquisto, attraverso l'applicazione di modelli di acquisto e standard contrattuali che, in linea con il quadro normativo vigente, valorizzino anche esperienze internazionali e sostenibilità ambientale, il presidio end-to-end dei processi di sviluppo delle gare e le attività amministrative connesse alle procedure di affidamento e agli strumenti di acquisto. Curare lo sviluppo delle iniziative di acquisto sotto soglia assicurandone l'assistenza legale.

Con riguardo all'organizzazione interna si riporta nel seguito l'organigramma della Società aggiornato al 31.12.2020.



Tutte le Divisioni aziendali di cui sopra riportano all'Amministratore Delegato della Società; le Divisione Internal Audit e la Divisione Compliance e Societario, così come l'Organismo di Vigilanza, il Dirigente preposto alla redazione dei documenti contabili societari e il Responsabile della prevenzione della corruzione e della trasparenza, riportano invece al Consiglio di Amministrazione, in ragione della necessaria autonomia ed indipendenza che deve caratterizzare tali funzioni.

L'organico della Società, al 31.12.2020, è costituito da n. 429 lavoratori dipendenti, di cui n. 35 dirigenti.

2.4 SISTEMA DELEGHE

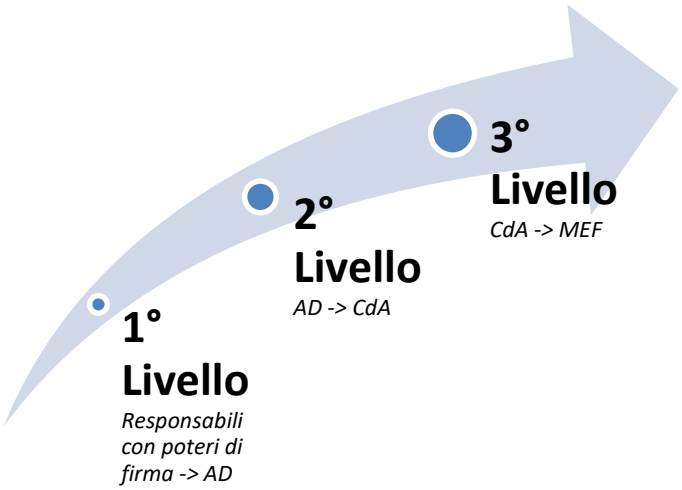
Il sistema delle deleghe attualmente in vigore in Consip ripercorre il quadro che emerge dall'Organigramma aziendale, come sopra riportato, sovrapponendosi ed integrandosi allo stesso.

La gestione dell'impresa spetta esclusivamente al Consiglio di Amministrazione, che compie le operazioni necessarie per l'attuazione dell'oggetto sociale in osservanza delle Direttive pluriennali impartite dal Dipartimento del Tesoro (MEF) in ordine alle strategie, al piano delle attività, all'organizzazione, alle politiche economiche, finanziarie e di sviluppo. Tali direttive sono emanate dal Dipartimento del Tesoro, sentite le altre Amministrazioni affidanti, e, per gli aspetti afferenti le attività svolte da Consip SpA in favore di Sogei SpA, ai sensi dell'articolo 4.1 lett. a), sentiti il Dipartimento delle Finanze e il Dipartimento dell'Amministrazione Generale, del Personale e dei Servizi. Le Direttive sono emanate entro il 30 novembre di ogni anno e preventivamente comunicate all'azionista ai fini della verifica dei profili economici e finanziari. Entro il 31 dicembre, in attuazione delle Direttive di cui sopra, gli Amministratori comunicano al Dipartimento del Tesoro un Piano generale annuale concernente le attività, gli investimenti e l'organizzazione.

All'Amministratore Delegato sono attribuiti poteri di corrente ed ordinaria amministrazione e poteri di rappresentanza della Società di fronte a qualunque autorità giudiziaria o amministrativa e di fronte a terzi, da esercitarsi nell'ambito degli indirizzi generali definiti dal CdA. In ragione delle specifiche esigenze della Società e tenuto conto della struttura organizzativa, l'A.D. ha a sua volta conferito procure ai responsabili delle Divisioni di I° livello aziendali, i quali possono, a loro volta, conferire procure nei limiti dei poteri loro assegnati, previa autorizzazione scritta dell'Amministratore Delegato stesso.

Il sistema di deleghe e dei poteri di firma, come sopra brevemente delineato, viene costantemente applicato e monitorato nel suo complesso, nonché - se e ove del caso - aggiornato in ragione delle modifiche intervenute nella struttura aziendale, in modo da corrispondere e risultare coerente con l'organizzazione gerarchico funzionale della Società. Vengono, dunque, attuati singoli aggiornamenti immediatamente conseguenti alla variazione di funzione, ruolo o mansione del singolo soggetto detentore del potere di firma, ovvero, laddove ritenuto necessario, periodici aggiornamenti che coinvolgono l'intero sistema.

Il sistema delle deleghe, prevede, inoltre, un triplice livello di reporting:



1° Livello – i responsabili delle Divisione di I livello possono esercitare le deleghe nei limiti delle attività svolte con riguardo alla Divisione di appartenenza e devono fornire un report periodico all'Amministratore Delegato in merito ad alcune tipologie di operazioni effettuate nell'ambito dei poteri – è in fase di elaborazione un sistema informatico per la gestione del sistema deleghe e il reporting all'A.D.

2° Livello – nell'ambito del generale obbligo di *accountability* degli organi delegati di cui all'art. 2381, co. 5 del codice civile e secondo quanto espressamente previsto dall'art. 15.5 dello statuto sociale, l'Amministratore Delegato riferisce al CdA e al Collegio sindacale con cadenza almeno trimestrale sull'andamento della gestione, sulla prevedibile evoluzione, nonché sulle operazioni di maggior rilievo effettuate dalla Società

3° Livello – ai sensi dell'art. 11.7 dello statuto sociale il CdA informa trimestralmente, attraverso rapporti sulla gestione e amministrazione, il Dipartimento del Tesoro (MEF) e l'azionista, i quali verificano, rispettivamente, *(i)* la rispondenza dell'azione sociale alle direttive impartite e al piano generale annuale e *(ii)* il mantenimento dell'equilibrio economico-finanziario.

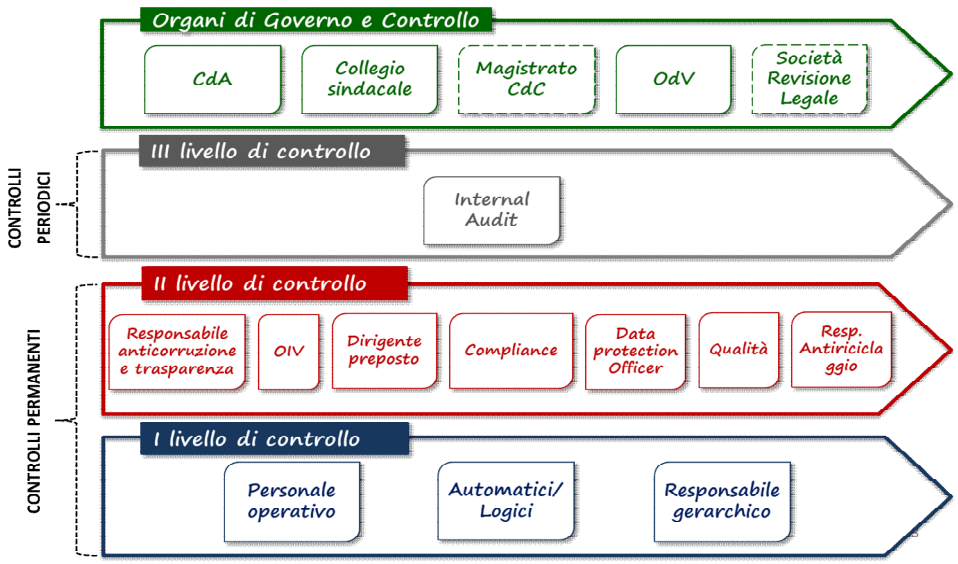
2.5 SISTEMA DEI CONTROLLI

Il sistema dei controlli interni (SCI) di Consip può essere definito come l'insieme delle regole, delle procedure e delle strutture organizzative che mirano ad assicurare il rispetto delle strategie e degli obiettivi aziendali ed il conseguente presidio delle aree di rischio.

Principi Generali del SCI	Obiettivi del SCI
✓ Separazione delle funzioni ✓ Segregazione dei compiti ✓ Attribuzione di ruoli e responsabilità ✓ Definizione delle linee di riporto ✓ Esistenza di regole di comportamento ✓ Proceduralizzazione delle attività e tracciabilità delle operazioni	✓ Conformità normativa ✓ Attendibilità e integrità del sistema informativo ✓ Efficienza e adeguatezza dei processi aziendali ✓ Salvaguardia del patrimonio sociale

Principi Generali del SCI	Obiettivi del SCI
✓ Istituzione esecuzione e documentazione di attività di controllo e vigilanza ✓ Esistenza di meccanismi di sicurezza che garantiscano adeguata protezione delle informazioni (accesso logico e fisico)	

Tale Sistema può essere suddiviso in tre distinti livelli, come rappresentato nel seguito.



2.5.a) Controlli di Linea - I livello -permanenti

Sono i controlli svolti direttamente dal personale operativo e descritti nelle procedure interne di riferimento. Ad essi si aggiungono i controlli logici previsti dagli applicativi informatici a supporto delle attività ed i controlli gerarchici svolti dai responsabili. Ogni operazione compiuta viene adeguatamente supportata a livello documentale, affinché sia possibile procedere, in ogni momento, agli opportuni controlli che attestino le caratteristiche e le motivazioni dell'operazione e ne individuino i soggetti rilevanti. Il personale Consip e ciascun soggetto operante a qualsiasi titolo per conto della Società viene sensibilizzato sulla necessità dei controlli, sull'esistenza delle norme e procedure applicabili, nonché sull'opportunità di un impegno attivo in prima persona per il migliore esito delle procedure di controllo.

2.5.b) Controlli di II Livello - permanenti

Sono i controlli sulla gestione dei rischi di impresa e di conformità alle norme. Hanno l'obiettivo di verificare il rispetto degli adempimenti normativi esterni e il presidio dei rischi contabili oltreché il monitoraggio gestionale. Rientrano in tale tipologia di controlli:

✓ *Compliance office*

La Società si è dotata di una Divisione Compliance e Societario (DCS), a diretto riporto del Consiglio di Amministrazione, che assicura il rispetto e la corretta implementazione delle

normative trasversali di interesse aziendale quali, a titolo di esempio, (i) il d.lgs. 231/01 in tema di responsabilità amministrativa delle persone giuridiche, (ii) la L. 190/12 in tema di anticorruzione, (iii) il D.Lgs. 33/13 in tema di trasparenza, (iv) il d.lgs. 231/07 in tema di antiriciclaggio, (v) la normativa in materia di protezione dei dati personali (GDPR – privacy); (vi) la normativa in materia di salute e sicurezza nei luoghi di lavoro ex d.lgs. 81/08.

Tra i compiti della Divisione rientra anche l'attività di supporto al Delegato del Datore di Lavoro (DDL) e ai diversi organi di controllo (CS - OdV – RPCT – DPO – GSOS – OIV) ai fini della gestione delle attività e dei programmi associati alle politiche attuate in ottemperanza alle normative sopra indicate, ivi incluse la valutazione degli impatti delle normative stesse e delle procedure interne, nonché l'individuazione, la valutazione e la gestione dei rischi.

✓ *Il Responsabile della prevenzione della corruzione e della trasparenza*

A far data dal 2014, la Società ha nominato il Responsabile della prevenzione della corruzione e della trasparenza (RPCT). Nel seguito una scheda riepilogativa dei principali compiti affidati al RPCT:

Anticorruzione L. 190/2012	o elabora/aggiorna la proposta di PTPC, che viene sottoposto al CdA e al Collegio Sindacale per la relativa adozione entro i termini di legge o verifica l'efficace attuazione del PTPC
Anticorruzione L. 190/2012	o definisce il Piano dei Controlli ex L. 190/12, coordinandosi con l'OdV, il DPO, il GSOS e l'IA ai fini della definizione del Piano Integrato dei Controlli o definisce il Piano di formazione integrato unitamente all'OdV, al GSOS e al DPO per quanto di interesse, con l'indicazione del personale da inserire o riferisce al CdA con cadenza almeno semestrale – il report viene inviato anche a Collegio sindacale, DP, OIV, DPO, GSOS e OdV o entro i termini di legge redige/pubblica in Società trasparente la Relazione annuale recante i risultati dell'attività svolta, da inviare al CdA e, per quanto di rispettiva competenza, anche a Collegio sindacale, DP, OIV, OdV, GSOS e DPO o riceve le relazioni periodiche del DP, dell'OIV, dell'OdV, del GSOS, del DPO e della Divisione di IA, unitamente agli esiti degli Audit e dei controlli effettuati o riceve le segnalazioni - ed effettua la relativa istruttoria - di cui al Sistema di whistleblowing o incontra periodicamente OdV, DP, OIV, DPO, GSOS e Collegio sindacale al fine di coordinare le rispettive attività o verifica, d'intesa con il responsabile della DRC ed unitamente all'OdV, l'effettiva applicazione del Programma Pluriennale di Rotazione adottato dal CdA o effettua le segnalazioni relative alle disfunzioni inerenti l'attuazione delle misure in materia di prevenzione della corruzione, così come definito nel PTPC
Trasparenza d.lgs 33/2013	o coordina gli aggiornamenti della sezione Trasparenza del PTPC o effettua una costante attività di controllo sull'adempimento da parte della Società degli obblighi di pubblicazione previsti dalla normativa vigente o effettua le segnalazioni relative alle disfunzioni inerenti l'attuazione delle misure in materia di trasparenza, così come definito nel PTPC o collabora con l'OIV al fine di garantire la necessaria sinergia

	o riceve l'attestazione dell'OIV valutando, all'esito, le eventuali azioni di competenza o controlla e assicura, unitamente ai Referenti per la trasparenza, la regolare attuazione dell'accesso civico in base di quanto stabilito dall'art. 5 d.lgs. 33/13 o gestisce le richieste di riesame di cui all'art. 5, comma 7, d.lgs. 33/2013 – anche con il supporto del DPO - decidendo con provvedimento motivato
Inconferibilità e incompatibilità d.lgs 39/2013	o vigila sul rispetto delle disposizioni di cui al d.lgs. 39/2013 in tema di inconferibilità e incompatibilità o gestisce il procedimento di accertamento e gli atti conseguenti di competenza, in ottemperanza alle Linee guida Anac in materia
Codice etico d.p.r. 62/2013	o collabora con l'OdV ai fini della diffusione della conoscenza e del monitoraggio sull'attuazione del Codice etico o riceve, unitamente all'OdV, le comunicazioni inerenti il conflitto di interessi reale e potenziale, fornendo alla Società il supporto necessario

Le funzioni attribuite al RPCT non sono delegabili se non in caso di straordinarie e motivate necessità, riconducibili a situazioni eccezionali. In considerazione della stretta connessione tra le misure adottate ai sensi del d.lgs. 231/2001 e il PTPC, le funzioni del RPCT devono essere svolte in costante coordinamento con quelle dell'OdV.

✓ *L'Organismo Indipendente di Valutazione o struttura analoga*

Le Linee guida ANAC per le società stabiliscono che *".....ad avviso dell'Autorità, ogni società attribuisce, sulla base di proprie valutazioni di tipo organizzativo, tali compiti all'organo interno di controllo reputato più idoneo ovvero all'Organismo di vigilanza (o ad altro organo a cui siano eventualmente attribuite le relative funzioni), i cui riferimenti devono essere indicati chiaramente nel sito web all'interno della sezione "Società Trasparente*". Stante i compiti normativamente attribuiti all'OdV, il CdA ha ritenuto opportuno confermare che l'organo di controllo interno più idoneo a svolgere i compiti assegnati all'OIV, sia il responsabile della Divisione Internal Audit, che è stato individuato quale soggetto cui affidare i compiti di attestazione dell'assolvimento degli obblighi di pubblicazione analogamente a quanto fanno gli OIV ex art. 14, comma, 4, lett. g), del D.Lgs 150/2009, per un periodo di tre anni fino all'approvazione del bilancio 2020.

Così come disposto dall'art. 1, comma 8bis, della L. 190/12 (introdotto dall'art. 41 del d.lgs.97/2016), sono attribuiti alla struttura analoga all'OIV delle società controllate le seguenti funzioni:

- verifica che i Piani triennali per la prevenzione della corruzione e della trasparenza siano coerenti con gli obiettivi stabiliti nei documenti di programmazione strategico-gestionale e che nella misurazione e valutazione delle performance si tenga conto degli obiettivi connessi all'anticorruzione e alla trasparenza;
- effettua l'attestazione degli obblighi di pubblicazione;
- riceve le segnalazioni aventi ad oggetto i casi di mancato o ritardato adempimento agli obblighi di pubblicazione da parte del RPCT.

A tal fine, l'OIV medesimo può chiedere al RPCT le informazioni e i documenti necessari per lo svolgimento del controllo e può effettuare audizioni di dipendenti. L'OIV riferisce all'ANAC sullo

stato di attuazione delle misure di trasparenza. A tal fine, entro i termini di legge, l'OIV pubblica l'attestazione sull'assolvimento degli obblighi di pubblicazione all'interno della sezione Società Trasparente, sotto-sezione Livello 1 "*Controlli e rilievi sulle società*" – sotto-sezione Livello 2 "*Attestazioni OIV o struttura analoga*".

✓ *Il Dirigente preposto alla redazione dei documenti contabili*

L'Azionista, con comunicazione del 22 novembre 2006 prot. n. 115828, ha disposto l'estensione in capo a Consip della disciplina di cui all'art. 154-bis del *Testo Unico delle disposizioni in materia finanziaria* (d.lgs. 58/1998), al fine di rafforzare i controlli sull'informativa economico-finanziaria della Società. Consip ha quindi proceduto, in sede di assemblea degli azionisti del 22 febbraio 2007, al relativo adeguamento statutario, inserendo l'art. 22-bis, che disciplina la figura del Dirigente Preposto alla redazione dei documenti contabili societari, con obblighi e responsabilità ai sensi di legge.

Lo statuto sociale stabilisce, dunque, che il Consiglio di Amministrazione debba nominare - previo parere obbligatorio del Collegio Sindacale - per un periodo non inferiore alla durata in carica del Consiglio stesso e non superiore a 6 esercizi, il Dirigente Preposto alla redazione dei documenti contabili societari, cui sono assegnati i compiti di:

a) predisporre adeguate procedure amministrative e contabili per la formazione del bilancio di esercizio;
b) attestare, unitamente agli organi amministrativi delegati della Società, con apposita relazione allegata al bilancio di esercizio, l'adeguatezza e l'effettiva applicazione delle procedure di cui sopra, nel corso dell'esercizio cui si riferiscono i documenti;
c) certificare la corrispondenza delle dichiarazioni contenute nei documenti societari alle risultanze dei libri e delle scritture contabili e la loro idoneità a fornire una rappresentazione veritiera e corretta della situazione patrimoniale, economica e finanziaria della Società.

In particolare, il Consiglio di Amministrazione di Consip ha provveduto a nominare il Dirigente Preposto alla redazione dei documenti contabili societari nella persona del responsabile della Divisione Amministrazione, Finanza e Controllo, conferendogli adeguati poteri e mezzi per l'esercizio dei suoi compiti, sia in termini di capacità decisionale, sia di capacità di spesa, tali da consentirgli un controllo effettivo sulla redazione dei documenti contabili societari. Inoltre, il Consiglio di Amministrazione ha approvato il *"Regolamento del Dirigente Preposto alla redazione dei documenti contabili societari",* volto a disciplinare l'operato del Dirigente anche nell'ambito della sua interazione con le altre strutture aziendali. Il DP riferisce al CdA con cadenza semestrale; la Relazione è trasmessa anche al Collegio sindacale, al RPCT e all'OdV nell'ottica di garantire le necessarie sinergie tra organi di controllo.

✓ *Data Protection Officer*

Il Regolamento UE/2016/679 - General Data Protection Regulation (nel seguito "Regolamento UE" o "GDPR") è entrato in vigore il 24 maggio 2016 ed è divenuto efficace per gli stati membri a partire dal 25 maggio 2018. In ottemperanza a quanto ivi indicato, il Consiglio di Amministrazione di Consip, in data 9 maggio 2018, ha provveduto a nominare il *Data Protection Officer*, il quale:

- supporta il Titolare in ogni attività connessa al trattamento dei dati personali

- vigila sull'osservanza del Regolamento UE e della normativa sulla protezione dei dati personali
- coopera con l'autorità Garante della protezione dei dati personali
- funge da punto di contatto per gli interessati per il trattamento dei loro dati o per l'esercizio dei loro diritti
- definisce il piano di formazione

Il DPO è individuato all'interno della Divisione Compliance e Societario (DCS) che assicura l'adeguamento alla normativa privacy e fornisce, pertanto, il relativo supporto al DPO stesso. Una volta nominato, il DPO si avvale anche del supporto tecnico del Comitato Data Protection, composto da:

- 2 risorse della Divisione E-Procurement e Sistemi Informativi, una per i Sistemi Informativi Interni e l'altra per la Piattaforma di e-procurement, al fine di garantire le attività di sviluppo e gestione di un programma di Information Security condiviso e uniforme all'interno dell'azienda;
- 1 risorsa della Divisione Pianificazione e Supporto Operativo – Area Modelli di Acquisto e Standard Documentali per la gestione delle tematiche privacy nell'ambito degli standard della documentazione di gara;
- 1 risorsa della Divisione ICT per il coordinamento nell'ambito delle gare del settore ICT;
- 1 risorsa della Divisione Sourcing Sanità Beni e Servizi per il coordinamento nell'ambito delle iniziative di gara in tale ambito merceologico
- 1 risorsa DCS per il supporto in tema compliance.

✓ *Responsabile Antiriciclaggio*

In ottemperanza all'art. 10 del d.lgs. 231/07, la cui applicazione è stata estesa anche alle P.A. e alle società da queste controllate, Consip ha nominato il Gestore delle segnalazioni delle operazioni sospette (GSOS) ed ha avviato il Progetto per l'implementazione del Modello interno di rilevazione, analisi e segnalazione delle operazioni sospette. Per la definizione di tale Modello Interno, è stata condotta un'attività di risk assessment sui rischi di riciclaggio e finanziamento del terrorismo, anche attraverso l'esame degli indicatori di anomalia emanati dall'UIF, adottandoli nella quasi totalità.

Il Modello SOS, realizzato in applicazione dell'approccio basato sul rischio e in coerenza con il principio di proporzionalità, si basa sull'adozione di processi e procedure dedicati e coerenti con l'articolazione societaria, la complessità e la dimensione aziendale, la tipologia dei servizi e prodotti offerti e le caratteristiche degli operatori economici, graduando l'intensità delle verifiche in relazione alla rischiosità degli stessi. Il Modello prevede inoltre l'adozione di un applicativo informatico per la gestione guidata dell'intero iter di segnalazione di operazione sospetta. L'utilizzo di tale applicativo assicura (i) omogeneità nell'esecuzione degli adempimenti operativi, (ii) tracciabilità delle verifiche svolte, (iii) monitoraggio dei tempi di esecuzione; (iv) inoltro delle comunicazioni all'UIF in via telematica; (v) riservatezza dell'identità dei segnalanti e del contenuto delle operazioni.

La Società si è inoltre dotata di apposita Policy interna per il governo dei rischi di riciclaggio e di finanziamento del terrorismo, provvedendo anche ad avviare programmi di formazione del personale dipendente.

✓ *Il Sistema di Gestione per la Qualità*

Consip è impegnata nel perseguire una politica ispirata ai principi della norma UNI EN ISO 9001. A tale scopo ha sviluppato, fin dall'ottobre 2010, un proprio Sistema di Gestione per la Qualità che ha connotato l'azienda come la prima centrale di committenza pubblica in Italia e fra le prime in Europa a ricevere la certificazione per i propri processi d'acquisto, vedendo così premiati gli sforzi sostenuti per garantire qualità, efficienza ed efficacia nell'organizzazione e nelle procedure e un costante orientamento alla soddisfazione del cliente.

La nuova edizione della UNI EN ISO 9001:2015 ha adottato un approccio per processi nella gestione aziendale basato sull'analisi e valutazione del rischio, con il fine ultimo di ottenere un miglioramento continuo dei processi e dei servizi offerti, oltre che assicurare la soddisfazione del cliente, in modo esplicito e misurabile.

Nel corso del 2019 si è provveduto al rinnovo triennale della certificazione ISO 9001:2015 del SGQ aziendale, estendendo il campo di applicazione – che già includeva Convenzioni, Accordi Quadro, Mepa e Sdapa – anche alle "acquisizioni su delega". In tal modo risultano certificate, ai sensi della norma ISO, tutte le attività di procurement dell'azienda, sia quelle relative al Programma di razionalizzazione degli acquisti sia quelle afferenti ad altri disciplinari. Il nuovo oggetto della certificazione è il seguente: *"Progettazione e sviluppo di iniziative per l'acquisizione di beni e servizi, in qualità di centrale di committenza, per la pubblica amministrazione".*

La Società si adopera affinché la Politica per la Qualità sia attuata e sostenuta a tutti i livelli dell'Organizzazione, assicurando la sua diffusione sia mediante comunicazioni aziendali mirate che mediante pubblicazione sulla intranet, in modo che sia conosciuta e compresa a tutti i livelli aziendali. Il Personale aziendale è direttamente coinvolto nelle attività ed ha la responsabilità dell'applicazione del Sistema di Gestione per la Qualità adottato, per quanto di competenza.

Periodicamente vengono effettuati audit interni al fine di accertare e garantire che il Sistema di Gestione per la Qualità sia:

- ✓ conforme a quanto pianificato, ai requisiti delle norme di riferimento e ai requisiti del Sistema di Gestione per la Qualità;
- ✓ efficacemente attuato e mantenuto aggiornato.

Le informazioni emerse dagli audit interni, oltre ad avviare Azioni Correttive immediate e mirate ai singoli processi o aree interessate, costituiscono uno strumento fondamentale per l'effettuazione del riesame del Sistema di Gestione per la Qualità. A tale scopo è predisposto un apposito Programma Annuale, che definisce le frequenze di audit in relazione allo stato e all'importanza dei processi e delle aree oggetto di verifica, nonché in relazione agli esiti delle precedenti verifiche. Gli audit interni sono svolti da personale competente, indipendente dall'attività lavorativa oggetto di verifica.

2.5.c) Controllo di III livello - periodico

✓ *Divisione Internal Audit*

In ottemperanza a quanto definito nello Statuto, la Società si è dotata di una Divisione Internal Audit (DIA) - a diretto riporto del Consiglio di Amministrazione - il cui Modello è stato approvato dal Consiglio di Amministrazione nel corso della riunione del 15 dicembre 2011.

L'Internal Auditing è un'attività indipendente ed obiettiva di assurance e consulenza, finalizzata al miglioramento dell'efficacia e dell'efficienza della Società. La mission della Divisione consiste, dunque, (i) nell'assistere la Società nel perseguimento dei propri obiettivi tramite un approccio professionale sistematico, finalizzato a valutare e migliorare i processi di gestione dei rischi, di governance e di controllo; (ii) nel portare all'attenzione del Consiglio di Amministrazione e dell'Alta Divisione i possibili miglioramenti alle politiche di gestione dei rischi, agli strumenti di misurazione ed alle procedure.

Consip adotta una gestione integrata dei controlli, così come meglio specificato ne successivo cap. 7.

2.5.d) Ulteriori controlli

In aggiunta a quanto sopra rappresentato, si richiamano gli ulteriori controlli effettuati dal Collegio sindacale, dalla società di revisione e dall'OdV ex d.lgs. 231/01 (cfr successivo cap. 5), oltre quello della Corte dei conti:

✓ *Corte dei conti*

Dal momento che Consip opera con risorse economiche esclusivamente pubbliche, un ulteriore controllo è esercitato dalla Corte dei conti ai sensi dell'articolo 12 della L. 259/1958, in merito alla gestione finanziaria e relativamente alle operazioni poste in essere nell'ambito della propria attività. In tale contesto la Corte dei conti delega periodicamente un Magistrato per il controllo, che ha il diritto di presenziare alle riunioni del Consiglio di Amministrazione ed a quelle del Collegio Sindacale e redige annualmente una Relazione sui risultati e le attività della Società.

Alla stessa Corte dei conti l'organo amministrativo e l'organo di controllo della Società sono tenuti a trasmettere periodicamente una serie di documenti aziendali e finanziari. In particolare, il Consiglio di Amministrazione di Consip deve trasmettere alla Corte dei conti:

- i conti consuntivi ed i bilanci di esercizio col relativo conto dei profitti e delle perdite corredati dalle relazioni dei rispettivi organi amministrativi e di revisione;
- copia dei verbali delle riunioni consiliari;
- copia dei contratti idonei a produrre effetti patrimoniali, economici o finanziari di elevato rilievo gestionale;
- copia degli atti e documenti contabili generali diversi dal bilancio di esercizio.

Il Collegio Sindacale della Società è tenuto invece a trasmettere alla magistratura contabile:

- le relazioni presentate in corso di esercizio;
- copia dei verbali delle sedute e dei controlli eseguiti, dei dati acquisiti e delle relazioni, raccomandazioni e giudizi formulati;
- copia delle relazioni di competenza.

✓ *Revisione legale dei conti*

Ai sensi dell'art. 22 dello Statuto sociale, la revisione legale dei conti della Società è esercitata da una società di revisione iscritta nell'apposito registro, individuata a seguito di procedura di gara, il cui incarico viene conferito direttamente dall'Assemblea degli azionisti.

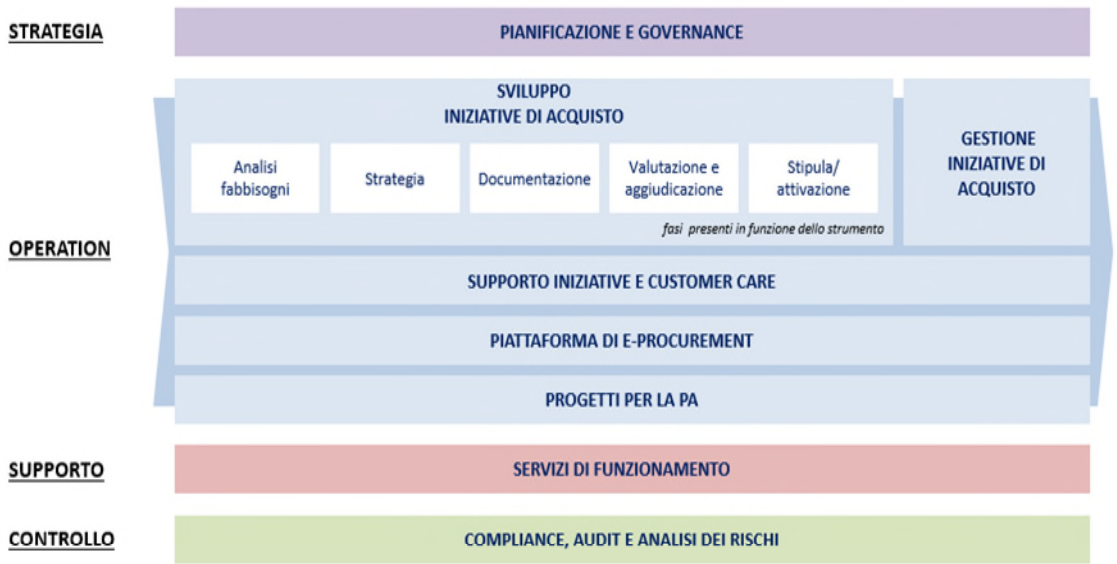
2.6 MAPPATURA DEI PROCESSI

Nell'ambito dell'organizzazione del lavoro della Società, una grande attenzione è rivolta allo sviluppo e al presidio dei processi aziendali, attraverso la progettazione (o riprogettazione) dei flussi di lavoro, il supporto alla implementazione operativa, e fino alla definizione dei documenti descrittivi. Con particolare riguardo alla mappatura dei processi vengono individuate otto tipologie di macro processi:

- pianificazione e governance
- sviluppo iniziative di acquisto
- gestione iniziative di acquisto
- supporto iniziative e customer care
- piattaforma di e-procurement
- progetti per la PA
- servizi di funzionamento
- compliance, audit e analisi dei rischi

articolati su quattro ambiti di raccordo:

1. strategia
2. operazioni
3. supporto
4. controllo

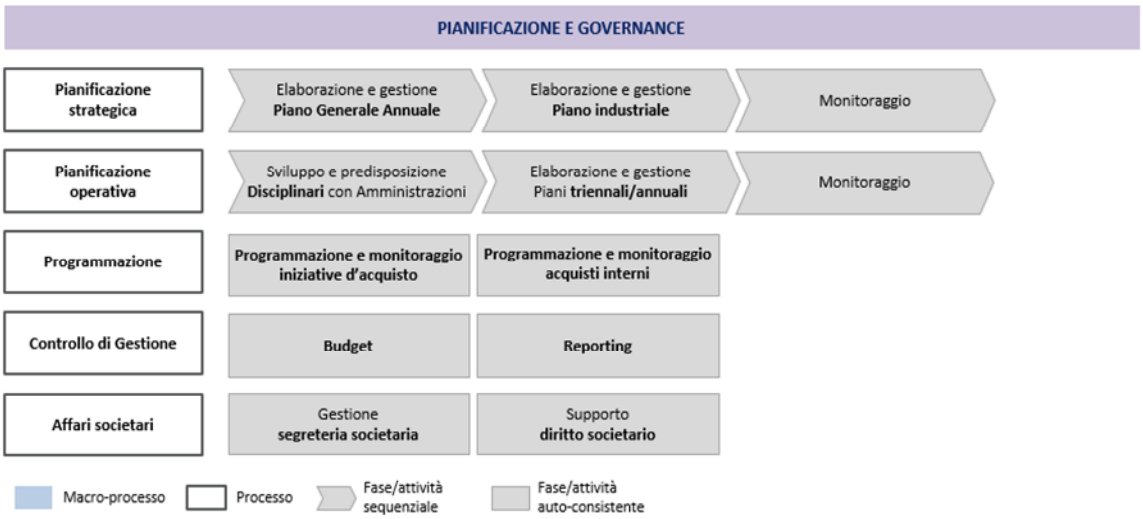


La Società ha, inoltre, creato un repository sulla intranet aziendale c.d. "Processi e Procedure", finalizzata a consentire una visione d'insieme dei processi, collocandoli in uno schema di riferimento, con l'obiettivo di diffondere e agevolare la comprensione e la conoscenza del modello dei processi e, quindi, accrescerne performance ed efficienza.

Nel seguito si riporta una descrizione sintetica dei processi e delle fasi contenuti nei macro processo.

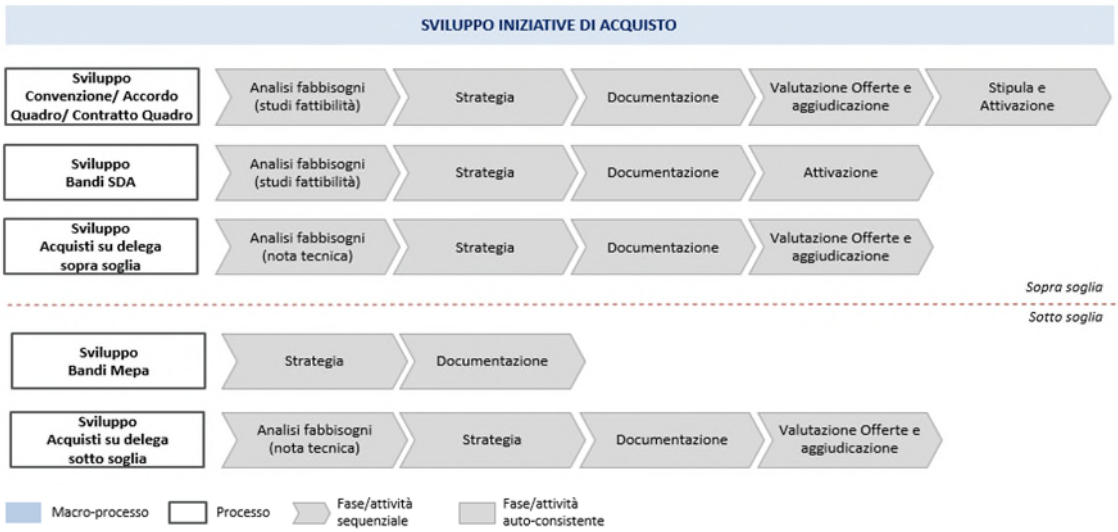
Processi di pianificazione e Governance

Processi di Governance volti a definire le strategie e le politiche per la gestione e il controllo delle attività poste in essere dall'azienda per il raggiungimento dei suoi obiettivi



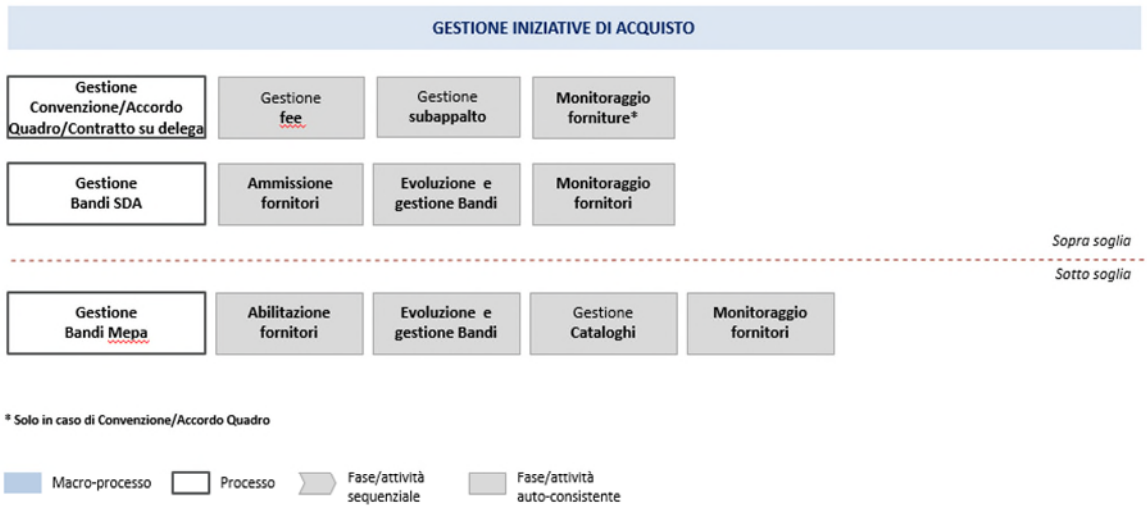
Sviluppo iniziative di acquisto

Processi relativi allo sviluppo delle iniziative di acquisto svolte al fine di supportare le Amministrazioni nella gestione dei propri acquisti di beni e servizi in attuazione della mission aziendale.



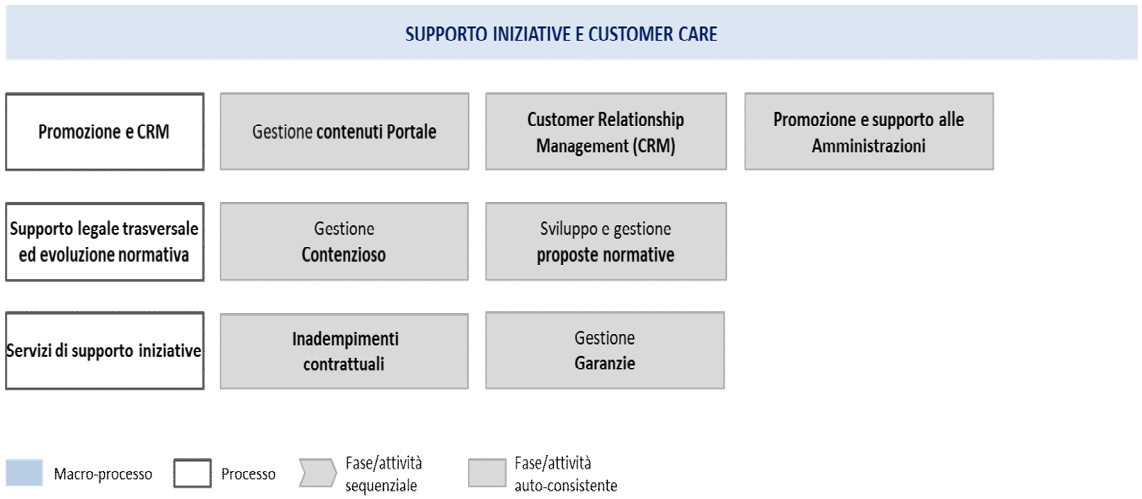
Gestione iniziative di acquisto

Processi relativi allo svolgimento delle attività connesse alla gestione degli output derivanti dalle iniziative di acquisto, nel rispetto delle condizioni contrattuali o delle regole di governo e monitoraggio della fornitura sempre nell'interesse della mission aziendale.



Processi di supporto iniziative e customer care

Processi che disciplinano le attività di customer relationship management e altre attività di supporto alla realizzazione e gestione delle iniziative di acquisto.



Processi relativi alla piattaforma di e-procurement

Processi relativi alla progettazione e allo sviluppo della piattaforma di e-Procurement, garantendone la gestione e l'evoluzione, nonché la sicurezza logica e fisica.

Progetti per la PA

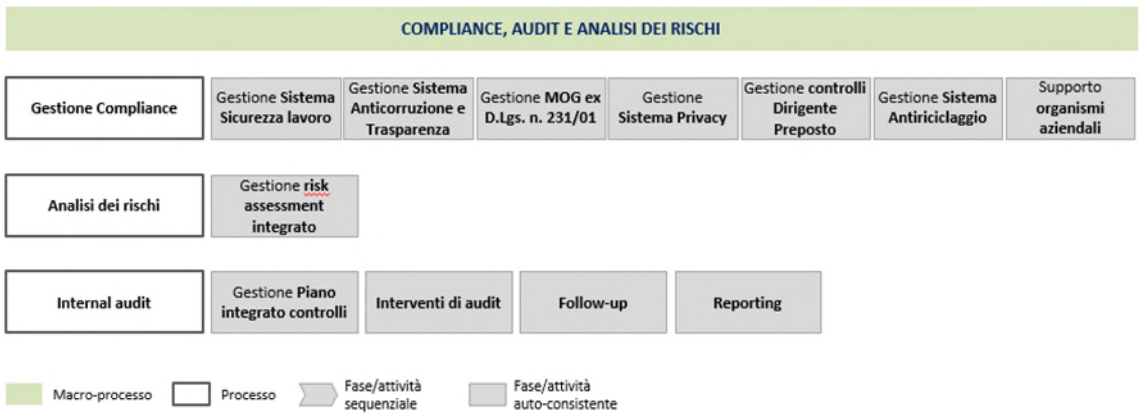
Processi che disciplinano il supporto specialistico per attività e progetti specifici svolti per le Amministrazioni di riferimento.

Servizi di funzionamento

Processi che contribuiscono indirettamente alla creazione dell'output supportando il regolare funzionamento e la valorizzazione delle attività aziendali.

Compliance, audit e analisi dei rischi

Sono tutti i processi che garantiscono, in coerenza con l'assetto regolamentare, le attività di presidio e controllo allo sviluppo delle attività della società.



CAPITOLO 3
IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO DI CONSIP SpA

3.1 PREMESSA: LE AZIONI POSTE IN ESSERE DA CONSIP E I PRINCIPI ISPIRATORI

Consip S.p.A., in coerenza con l'impegno sempre profuso nella creazione e nel mantenimento di un sistema di *governance* caratterizzato da elevati standard etici e da un'efficiente gestione dell'attività aziendale, sin dagli anni immediatamente successivi all'entrata in vigore della normativa ha svolto le necessarie attività di adeguamento al Decreto.

La prima versione del Modello di Organizzazione, Gestione e Controllo prescritto dall'articolo 6, comma 1, lett. a) del Decreto (il "**Modello**") è stata approvata con delibera del Consiglio di Amministrazione di Consip del 13 ottobre 2003, cui sono seguiti diversi aggiornamenti; sempre nel 2003è stato altresì nominato l'Organismo preposto all'attività di vigilanza e controllo sul funzionamento e l'osservanza del Modello stesso (l'"**Organismo di Vigilanza**" o "**OdV**").

In considerazione delle modifiche apportate all'organizzazione aziendale e dell'introduzione di nuovi reati presupposto nell'ambito del Decreto[30], Consip ha ritenuto opportuno avviare un procedimento di complessiva e organica revisione ed aggiornamento del Modello e della sua impostazione, che recepisse anche la "compliance integrata" adottata dalla Società sia con riguardo al risk assessment che ai controlli ed alla formazione. Preso atto della cospicua giurisprudenza penale formatasi in materia, il procedimento ha coinvolto ogni aspetto del Modello, nelle sue varie componenti strutturali e modalità applicative, così da attuare anche la necessaria integrazione con il Piano Triennale della Prevenzione della Corruzione (PTPC) e tra i relativi organi di controllo (cfr successivo par. 3.2).

Nelle attività di aggiornamento del Modello, si è altresì tenuto conto delle indicazioni contenute:

- nelle "*Linee Guida per la costruzione dei modelli di organizzazione, gestione e controllo ex D.Lgs. n. 231/2001*" di Confindustria;
- nelle circolari ABI serie legale n. 16 del 22 maggio 2002 e n. 2 del 27 gennaio 2003 in merito alle "*Linee Guida ABI per l'adozione di modelli organizzativi da parte della Banche*";
- del "*Position Paper*" dell'Associazione Italiana Internal Auditors datato ottobre 2001;
- della Circolare n. 68 del 19 novembre 2002 di *Assonime*;
- delle Linee guida UNI/INAIL per un sistema di gestione della salute e sicurezza nei luoghi di lavoro (SGSL) del 28 settembre 2001;
- del documento "*Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza, prospettive di revisione del d.lgs. 8 giugno 2001 n. 231"* elaborato a febbraio 2019 dal Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili insieme ad ABI, al Consiglio Nazionale Forense e Confindustria.

* * *

Il Modello, nell'esprime la volontà di Consip di adottare tutte le misure necessarie affinché

[30] Delitti in materia di discriminazione razziale e xenofobia richiamati dall'art. 25 – *terdecies* ed i reati cosiddetti tributari, richiamati dall'art. 25 - *quinquiesdecies*

l'attività svolta dalla Società sia improntata al rispetto della legge e sia ispirata a principi di correttezza, trasparenza e tracciabilità, mira a garantire che tutte le attività:

a. siano poste in essere in perfetta osservanza delle leggi e dei regolamenti vigenti, nonché delle procedure interne e dei principi comportamentali dettati dal Codice Etico adottato dalla Società;
b. perseguano finalità lecite e non mirino a far conseguire vantaggi illeciti alla Società o suoi rappresentanti o dipendenti;
c. siano motivate, documentate e quindi controllabili.

Eventuali divergenze del Modello rispetto a talune specifiche indicazioni delle associazioni di categoria, se presenti, non inficiano la correttezza di fondo e la validità del Modello stesso. Tali direttive, infatti, hanno per definizione carattere generale, laddove il Modello deve essere predisposto con riferimento alla realtà concreta dell'ente.

Il Modello non mira ad una sostituzione incondizionata ed invasiva del complesso rappresentato dalle direttive aziendali e dalle procedure operative già esistenti presso la Società con un nuovo apparato di prescrizioni comportamentali e regole di controllo autoreferenziale "calato dall'alto" sulla struttura organizzativa dell'ente. Al contrario, l'approccio che si è adottato nel predisporre il Modello ha inteso privilegiare la valorizzazione dei presidi organizzativi esistenti, nella misura in cui essi si mostrino adeguati allo scopo di prevenzione della commissione dei reati-presupposto, che Consip persegue con l'adozione ed attuazione del Modello stesso. Tale soluzione ha permesso di evitare un eccessivo ed inutile appesantimento del corpo normativo aziendale attualmente in vigore, che avrebbe condotto, in ultima analisi, a risultati inefficaci se non controproducenti, consentendo, invece, di procedere con interventi mirati e quanto più possibile coerenti con il suddetto corpo normativo interno dell'ente, soltanto laddove l'analisi dell'esistente rendesse evidente la necessità di rinforzare l'azione penal-preventiva in relazione a determinate aree di attività, rivelatesi non adeguatamente presidiate.

Il Modello ha quindi individuato una serie di protocolli preventivi, finalizzati a prevenire il rischio di commissione di reati-presupposto all'interno di Consip, cui le procedure/linee guida interne si devono rigorosamente ispirare, andando a codificare le singole misure preventive già attuate e gli eventuali interventi correttivi da attuare nell'ambito dei processi interni, coordinandosi a tal proposito con il PTPC. Insieme a tali protocolli, è stato inoltre predisposto un apparato sanzionatorio posto a presidio delle regole, procedure e protocolli facenti capo al Modello e al PTPC.

Il Modello, inoltre, formalizza e chiarisce l'attribuzione di responsabilità, le linee di dipendenza gerarchica e la descrizione dei compiti operativi, con specifica previsione di principi generali di controllo quali, ad es., la segregazione delle funzioni coniugata con opportuni meccanismi di controllo reciproco: unitamente al PTPC, rappresenta, dunque, un sistema strutturato ed organico di processi, procedure ed attività di controllo (preventivo ed *ex post*), che coinvolge ogni aspetto dell'attività della Società.

3.2 IL MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. N. 231/2001 E IL PIANO ANTICORRUZIONE

Nonostante alcune evidenti analogie, il d.lgs. 231/01 (il "Decreto") e la L. 190/2012 (la "Legge) differiscono sensibilmente, soprattutto con riguardo al concetto di corruzione. Il Decreto considera, infatti, un'elencazione tassativa dei reati presupposto da prevenire, commessi nell'interesse o a vantaggio della Società, mentre la Legge fa riferimento ad un concetto più ampio di "corruzione", in cui rilevano non solo l'intera gamma dei reati contro la P.A. disciplinati dal Titolo II del Libro II del codice penale, ma anche le situazioni di "cattiva amministrazione" *("maladministration")*, nelle quali vanno compresi tutti i casi di deviazione significativa, in cui gli interessi privati condizionano il corretto operare dell'Amministrazione/Ente.

Tale concetto è richiamato anche nel PNA 2019, laddove viene ribadito che:

- il d.lgs. 231/01 ha riguardo ai reati commessi nell'interesse o a vantaggio della società o che comunque siano stati commessi anche e nell'interesse di questa, riferendosi pertanto alle fattispecie tipiche di concussione, induzione indebita a dare o promettere utilità e corruzione, nonché alla corruzione tra privati;
- la L. 190/12, di contro, è finalizzata a prevenire anche reati commessi in danno della Società.

In passato il PNA 2013, per evitare inutili ridondanze, aveva stabilito che, qualora in una società fosse già stato adottato il Modello di organizzazione e gestione ex d.lgs. 231/01, nella propria azione di prevenzione della corruzione si potesse "fare perno" su esso, estendendone l'ambito di applicazione non solo ai reati contro la Pubblica Amministrazione previsti dal d.lgs. 231/01, ma anche a tutti quelli considerati nella L. 190/12, dal lato attivo e passivo, anche in relazione al tipo di attività svolto dall'ente. Tale impostazione è stata poi confermata dal "*Documento condiviso dal Ministero dell'economia e delle finanze e dall'ANAC per il rafforzamento dei meccanismi di prevenzione della corruzione e di trasparenza nelle società partecipate e/o controllate dal Mef"* di dicembre 2014, nel quale veniva chiaramente ribadito come le misure contemplate dalla L. 190/2012 dovessero trovare applicazione per le società controllate dal Ministero dell'Economia e delle Finanze, anche nei casi in cui le stesse avessero già adottato il Modello previsto dal d.lgs. 231/2001, in quanto l'ambito di applicazione dei due interventi normativi sopra menzionati non coincideva: "*Difatti, mentre le norme contenute nel d.lgs. 231/2001 sono finalizzate alla prevenzione di reati commessi nell'interesse o a vantaggio della società, la L. 190/2012 persegue la finalità di prevenire condotte volte a procurare vantaggi indebiti al privato corruttore in danno dell'ente (nel caso di specie, della società controllata). Ne consegue che le società controllate, che abbiano già approvato un Modello di prevenzione dei reati della specie di quello disciplinato dal d.lgs. 231/2001, devono integrarlo con l'adozione delle misure idonee a prevenire anche altri fenomeni di corruzione e illegalità all'interno delle Società, come indicati dalla L. 190/2012*".

Successivamente gli Indirizzi Mef e le Linee guida ANAC per le società hanno ribadito quanto sopra, formalizzando l'obbligo di integrare il Modello ex d.lgs. 231/01 con l'adozione delle misure idonee a prevenire anche i fenomeni corruttivi e di illegalità all'interno delle società: tali misure dovevano costituire, appunto, il Piano di prevenzione della corruzione. In tale contesto il Consiglio di Amministrazione di Consip, accogliendo il suggerimento del PNA 2013, nel 2015 aveva optato

per la definizione di un Piano Triennale per la prevenzione della corruzione e di un Programma per la trasparenza e l'integrità, successivamente riuniti nell'attuale PTPC.

Nel novembre 2017, le Linee Guida ANAC 2017 per le società hanno previsto la possibilità di accorpare, in un unico documento, le misure di prevenzione della corruzione/trasparenza, trasfuse nel PTPC, e i presidi contenuti nel Modello di organizzazione, *ex* d.lgs. 231/2001, riservando, tuttavia, alle prime un'autonoma "*sezione*". Le Linee Guida lasciano impregiudicata la facoltà di mantenere distinti i due strumenti di prevenzione, in considerazione delle differenze di impostazione[31].

Data la centralità del rischio di corruzione passiva all'interno di Consip e le diverse responsabilità ascrivibili rispettivamente al RPCT e all'OdV, si è per il momento ritenuto preferibile tenere separati il PTPC e il Modello 231, curando il coordinamento funzionale tra gli stessi. Pertanto, quanto indicato nel PTPC, con particolare riguardo alle misure preventive della corruzione e della cattiva amministrazione, alla formazione ed alle misure di monitoraggio e di vigilanza sull'attuazione degli obblighi previsti nel Piano stesso, ivi inclusi quelli in tema di trasparenza, è elaborato in coordinamento e ad integrazione dei contenuti del Modello ex d.lgs. 231/01. Ed infatti, al fine di garantire un'azione sinergica fra il Modello e il PTPC:

- viene effettuato un *risk assessment* integrato;
- le prescrizioni e i Piani di azione identificati nel PTPC sono considerati, ove applicabili, come presidi di controllo relativi alla prevenzione delle fattispecie di reato ex d.lgs. 231/2001 e costituiscono nuovi protocolli di controllo;
- l'integrazione è garantita anche a livello di controlli, attraverso il Piano Integrato dei Controlli (PIC), e nell'ambito della formazione, attraverso il Piano Integrato della Formazione;

come meglio specificato nei singoli capitoli dedicati.

Nell'espletamento dei propri compiti l'OdV e il RPCT operano in costante collaborazione, garantendo, dunque, il necessario coordinamento.

3.3 STRUTTURA DEL MODELLO

Il Modello è costituito da una "Parte Generale" e da una serie di "Parti Speciali" predisposte per le diverse categorie di reato contemplate nel Decreto e considerate a rischio per la Società, cui sono allegate le relative schede rischio.

3.3.a) Struttura della Parte Generale

La Parte Generale del Modello individua gli elementi essenziali della struttura organizzativa della Società e del sistema dei controlli, andando a definire la funzione, i contenuti e le modalità per la

[31] ANAC Delibera n. 1134 del 08/11/2017, Par. 3.1.1. "*Queste misure devono fare riferimento a tutte le attività svolte ed è necessario siano ricondotte in un unico documento unitario che tiene luogo del Piano di prevenzione della corruzione anche ai fini della valutazione dell'aggiornamento annuale e della vigilanza dell'ANAC. Se riunite in un unico documento con quelle adottate in attuazione del d.lgs. 231/01, dette misure sono collocate in una sezione e dunque chiaramente identificabili, tenuto conto che ad esse sono correlate forme di gestione responsabilità differenti*".

gestione del Modello stesso.

Nello specifico contiene:

a. la descrizione del quadro normativo in vigore;

b. la rappresentazione sintetica della struttura organizzativa e delle attività svolte da Consip, con particolare attenzione al sistema dei controlli ed alla mappatura dei processi;

c. le modalità per la redazione, aggiornamento ed implementazione del Modello;

d. la metodologia utilizzata per l'analisi integrata dei rischi e per la trattazione dei rischi stessi;

e. le regole sulla costituzione dell'OdV, ivi incluse le relative caratteristiche ed i compiti;

f. la descrizione del sistema di whistleblowing;

g. il sistema di Monitoraggio del Modello ed il Piano Integrato dei Controlli;

h. le regole che disciplinano le modalità di diffusione del Modello, ivi inclusi i piani di formazione;

i. focus sulle principali misure preventive trasversali/protocolli quali ad esempio: (i) la gestione delle situazioni di conflitto di interessi; (ii) il principio della segregazione dei compiti e delle funzioni, cui sono ispirate tutte le procedure aziendali adottate dalla Società; (iii) la rotazione delle risorse, con particolare attenzione ai ruoli rivestiti dai dipendenti Consip nell'ambito delle procedure di gara (es. commissari di gara, RdP, ecc); (iv) la riservatezza, ecc.;

j. le sanzioni applicabili in caso di violazioni delle regole e delle prescrizioni contenute nel Modello e nel PTPC, disciplinate nel dettaglio all'interno dell'allegato "Sistema Disciplinare";

k. Matrice "Rischi Reato/Referenti" contenente l'elenco dei reati presupposto che, a livello teorico, è possibile siano commessi dai Destinatari con indicazione dei relativi Referenti aziendali responsabili dell'attività a rischio e, dunque, dell'effettiva applicazione dei presidi di controllo posti in essere;

l. Matrice delle Attività Rischio Reato contenente la mappatura delle aree a rischio, associate alle fattispecie di reato con esempi di possibili modalità di realizzazione dei reati e dei macro processi strumentali/funzionali potenzialmente associabili, unitamente all'identificazione delle Parti Speciali del Modello a cui sono associate le rispettive attività a rischio.

3.3.b) Struttura delle Parti Speciali

Le Parti Speciali del Modello contengono una descrizione relativa a:

a. le diverse fattispecie di reato-presupposto concretamente e potenzialmente rilevanti in azienda, individuati in ragione delle caratteristiche peculiari dell'attività svolta da Consip;

b. le attività a rischio-reato caratteristiche della singola Parte speciale;

c. i processi/attività ritenuti a rischio di commissione di uno dei reati previsti dal Decreto;

d. i princìpi comportamentali a cui devono conformarsi i destinatari del Modello;

e. i presidi di controllo di cui la Società si è dotata per prevenire i rischi individuati.

Ogni parte speciale è inoltre corredata delle singole schede rischio (cfr successivo cap. 4.4), allegate anche al PTPC, che, per ogni evento di rischio riportano dettagliatamente:

- ✓ *Anagrafica evento rischio*: (i) attività a rischio e descrizione; (ii) Risk owner, contributor; (iii) Macro processo, Processo e Fase; (iv) Area e Sotto Area;
- ✓ *Dettaglio rischio*: (v) Fattori abilitanti; (vi) Conseguenze; (vii) Riferimenti normativa esterna ed interna; (viii) Anomalie significative; (ix) Indicatori di rischio;
- ✓ *Controlli*: (x) Sintesi misure di controllo; (xi) Misure generali; (xii) Misure specifiche.
- ✓ *Piani di azione*: sintesi degli interventi correttivi da implementare, monitorati dal RPCT.

3.4 Rilievi preliminari sulle principali aree di esposizione di Consip ai rischi di commissione di reati-presupposto

Con il progressivo ampliarsi del campo di applicazione della normativa in questione, il grado di *sensibilità* di Consip alle problematiche relative alla corretta prevenzione dei reati-presupposto è via via aumentato.

Limitando la riflessione alle più rilevanti aree di esposizione della Società a rischi connessi al Decreto, occorre comunque considerare che:

a) a causa dei rapporti intrattenuti con le Pubbliche Amministrazioni, tra l'altro anche nella qualità di stazione appaltante, Consip è particolarmente esposta al rischio di commissione dei reati contro la P.A. richiamati dagli artt. 24 e 25 del Decreto;

b) la natura di impresa in forma di società per azioni espone Consip, al pari di qualsiasi altra società commerciale, al rischio di commissione dei c.d. *reati societari* di cui all'art. 25-*ter* del Decreto;

c) l'introduzione dell'art. 24-*bis* in materia di delitti informatici e trattamento illecito di dati ha sicuramente ampliato l'area di potenziale esposizione a rischi (in aggiunta alla originaria area esposizione a rischi di commissione del reato di frode informatica di cui all'art. 640-*ter* c.p.)[32];

d) con l'introduzione dell'art. 25-quinquiesdecies in materia di reati tributari è venuta a svilupparsi un'ulteriore ampia area di potenziale esposizione a rischi, che ha portato all'individuazione di nuovi rischi specifici nel settore di riferimento, in aggiunta a quelli già

[32] Tale ampliamento del perimetro relativo all'area di esposizione al rischio della Società ha interessato, in particolare: (i) le attività informatiche svolte da Consip per le Amministrazioni dello Stato, ove previsto dalla legge, con particolare riguardo alle attività in materia finanziaria e contabile, a favore del Ministero dell'Economia e delle Finanze e della Corte dei conti, ai sensi del d.lgs. 414/1997 e sulla base della *Convenzione per la realizzazione e gestione delle attività informatiche dello Stato* attualmente in vigore ("*Convenzione ICT*"); (ii) una serie di attività relative alla realizzazione e gestione di un apposito sistema di *e-procurement* dedicato all'applicazione in via telematica delle c.d. *Convenzioni* con la Pubblica Amministrazione *ex* artt. 26 Legge n. 488/1999 e 58 Legge n. 388/2000 (nell'ambito del programma di Razionalizzazione della spesa pubblica), all'espletamento di gare telematiche, nonché alla predisposizione del mercato elettronico della Pubblica Amministrazione (c.d. *marketplace*)

esistenti.

Le considerazioni di carattere generale appena svolte non esauriscono la trattazione delle aree di rischio peculiari della struttura organizzativa e delle attività svolte da Consip, con riferimento a tutte le categorie di fattispecie criminose rilevanti *ex* Decreto. In questo senso, le risultanze –del risk assessment integrato costituiscono la base metodologica del lavoro di predisposizione del presente Modello e trovano materiale collocazione nelle apposite sezioni descrittive delle singole Parti Speciali.

Si evidenzia infine che non sono state redatte le Parti Speciali inerenti i seguenti reati presupposto, in quanto il rischio di commissione degli stessi a vantaggio o nell'interesse della Società non è stato ritenuto configurabile considerata l'attività dalla stessa svolta:

- ✓ Falsità in monete, in carte di pubblico credito, in valori di bollo e in strumenti o segni di riconoscimento (art. 25-bis);
- ✓ Reati con finalità di terrorismo o di eversione dell'ordine democratico previsti dal codice penale e dalle leggi speciali (art. 25-quarter);
- ✓ Pratiche di mutilazione degli organi genitali femminili (art. 25-*quater1*)
- ✓ Delitti contro la personalità individuale (art. 25-*quinquies*);
- ✓ Frode in competizioni sportive, esercizio abusivo di gioco o di scommessa e giochi d'azzardo esercitati a mezzo di apparecchi vietati (art. 25 – *quaterdecies*);
- ✓ Reati di contrabbando (art. 25 – s*exiesdecies*);
- ✓ Reati in materia di sostanze alimentari, rilevanti solo per gli enti che operano nell'ambito della filiera degli oli vergini di oliva (Legge 9/2013).

Nell'ambito delle Parti Speciali, inoltre, l'individuazione dei singoli rischi non ha tendenzialmente tenuto conto del concetto di "interesse" e di "vantaggio" (salvo nei casi di particolare evidenza), in analogia con le *best practice* in materia, così da adottare un approccio il più estensivo possibile nell'ottica di evitare erronee omissioni o di contenere eccessivamente il campo di applicazione.

3.5 Il Codice Etico

Consip opera secondo principi etici diretti ad improntare lo svolgimento dell'attività, il perseguimento dello scopo sociale e la crescita della Società stessa nel rispetto delle leggi vigenti. A tale fine, la Società si è dotata di un codice etico (cfr allegato "Codice Etico"), volto a definire una serie di princìpi di "*deontologia aziendale*" riconosciuti come propri e dei quali esige l'osservanza da parte dei propri organi societari, dei dipendenti e di tutti coloro che cooperano a qualunque titolo al perseguimento dei fini aziendali.

Il Codice completa il Modello e il PTPC ed è destinato a tutti i dipendenti e collaboratori, senza alcuna eccezione, ed a tutti coloro che, direttamente o indirettamente, stabilmente o temporaneamente, instaurano rapporti o relazioni con Consip ed operano per perseguirne gli obiettivi.

Entrambi gli strumenti perseguono, nella loro concreta attuazione, un obiettivo comune: salvaguardare il rispetto della legalità nell'operato aziendale, anche a prescindere da possibili situazioni di responsabilità contestate ai suoi esponenti. Ogni soggetto a cui si applicano i precetti contenuti in tali documenti è consapevole che, in nessun caso, l'intenzione di agire nell'interesse o a vantaggio di Consip giustifica il compimento di atti e comportamenti in contrasto con le prescrizioni del Modello, del PTPC e del Codice Etico, ai quali deve riconoscersi valore indisponibile, prioritario ed assoluto.

Consip è impegnata nella effettiva e capillare diffusione delle informazioni relative a normative e regole comportamentali che devono essere rispettate al fine di assicurare che l'attività della Società si svolga nel rispetto dei canoni dettati dal Codice Etico[33] e dalla normativa vigente. Il Codice è dunque pubblicato nella intranet aziendale e sul sito internet in Società trasparente, nella sezione "Disposizioni generali" sottosezione "Atti generali", allo scopo di darne la massima diffusione. Inoltre, al fine di garantirne l'effettivo rispetto, il Codice (i) è espressamente richiamato in tutti i contratti stipulati dalla Società e (ii) in specifiche dichiarazioni che gli amministratori, i sindaci, i consulenti, i commissari di gara, i Responsabili del procedimento e i dipendenti, all'atto dell'assunzione/sottoscrizione del contratto, devono rilasciare, impegnandosi a rispettare i principi ivi contenuti, con particolare riguardo a quelli inerenti la riservatezza ed il conflitto di interessi. Eventuali violazioni sono sanzionabili in base al Sistema disciplinare della Società.

Le regole dettate dal Codice non sostituiscono ma integrano i doveri fondamentali dei dipendenti già fissati nel C.C.N.L..

Consip ribadisce il carattere di cogenza e precettività del Codice Etico e la possibilità per la Società di irrogare sanzioni disciplinari commisurate alla gravità delle eventuali infrazioni accertate al pari delle violazioni al Modello e del PTPC, come meglio indicato nel Sistema Disciplinare della Società.

Il compito di vigilare sulla corretta e costante applicazione in azienda del Codice Etico viene affidato all'Organismo di Vigilanza e al Responsabile della prevenzione della corruzione e della trasparenza di Consip, che operano in stretta sinergia.

3.6 TERMINI E MODALITÀ DI ADOZIONE E DI AGGIORNAMENTO DEL MODELLO E DEL CODICE ETICO DA PARTE DEGLI ORGANI DI VERTICE

3.6.a) Gruppo di lavoro

Per la redazione/aggiornamento del Modello e/o del Codice Etico può essere costituito un gruppo di lavoro, coordinato dalla DCS, composto dai *Focal Points* individuati dai responsabili delle Divisioni (Referenti), con lo scopo di fornire, ciascuno per le materie di rispettiva competenza di

[33] Delibera ANAC n. 177 del 19 febbraio 2020 - La elaborazione di principi etici costituisce un elemento essenziale del sistema di controllo per la prevenzione dei reati previsto dal d.lgs. n. 231 del 2001, configurandosi quale importante presidio di prevenzione rispetto alla commissione di illeciti. Tali principi sono inseriti in un codice etico, da considerarsi parte integrante del "modello 231", che contiene l'insieme dei doveri e delle regole comportamentali che vincolano i soggetti che, a qualunque livello, operano all'interno dell'ente nei confronti dei portatori di interesse.

volta in volta ritenute necessarie, il relativo supporto. Ciò anche al fine di garantire il coinvolgimento di tutti gli uffici interessati alle tematiche ivi contenute, condividerne l'impianto strutturale e raccogliere i contributi e le proposte per la definizione delle misure di prevenzione della corruzione e per la loro implementazione.

E' infatti compito dei *Focal Points* condividere con il rispettivo Referente e le strutture di appartenenza le attività svolte dal Gruppo di lavoro, al fine di raccogliere e sottoporre alla DCS eventuali criticità o proposte migliorative.

Il Gruppo di lavoro può variare la propria composizione a seconda delle esigenze che si dovessero manifestare, estendendo la partecipazione anche a più risorse della medesima Divisione ai fini di una più ampia cooperazione.

Il Gruppo di lavoro può essere altresì coinvolto nelle attività successive all'adozione del Modello da parte del Consiglio di Amministrazione, al fine di stimolare le necessarie riflessioni e gli opportuni confronti tesi a migliorare i contenuti del Piano.

3.6.b) Adozione del Modello da parte degli Organi di Vertice

Una volta effettuate le necessarie condivisioni:

(i) con i soggetti intervistati ed i relativi *Focal Points* per quanto riguarda l'analisi e la gestione dei rischi (cfr. cap. 4.3)

(ii) con l'OdV per quanto riguarda il Modello complessivamente inteso

il responsabile della DCS sottopone il Modello e/o il Codice Etico al Consiglio di Amministrazione in tempo utile per consentirne un'accurata disamina e l'approvazione entro la prima riunione utile.

3.6.c) Modalità di aggiornamento

Modello e/o il Codice Etico vengono aggiornati in relazione a modifiche e/o integrazioni che si dovessero rendere necessarie, in particolare in conseguenza di:

modifiche normativa	o intervento di modifiche normative o di evoluzioni giurisprudenziali e dottrinali di interesse
modifiche organizzazione	o modifiche dell'assetto organizzativo e/o delle responsabilità in capo alle singole funzioni aziendali o mutamenti nelle attività svolte dalla Società
risk assessment	o identificazione di nuove attività a rischio o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività o risultanze del risk assessment integrato

segnalazione ambiti di miglioramento	o riscontro di carenze e/o lacune nelle previsioni del Modello e/o del Codice Etico a seguito di (i) verifiche sull'efficacia del medesimo, occasionali o svolte dall'OdV; (ii) segnalazioni/verifiche svolte dal RPCT, dal DP, dal DPO, dal GSOS o dalla Divisione IA; (iii) segnalazioni provenienti da altri organi, dipendenti o terzi; (iv) segnalazioni provenienti dalle RSU o significative violazioni delle prescrizioni del Modello e/o del Codice Etico complessivamente inteso o del PTPC

Modifiche normativa

La DCS cura gli interventi necessari monitorando le evoluzioni normative e giurisprudenziali, anche con il supporto della DAL, che segnala tempestivamente le modifiche delle disposizioni normative e/o le evoluzioni giurisprudenziali o dottrinali in tema di anticorruzione o di trasparenza.

La DCS verificata la necessità di aggiornamento del Modello e/o Codice Etico con l'OdV, avvia le attività di approfondimento e, successivamente, di redazione/integrazione con il supporto del gruppo di lavoro, se necessario.

Il documento finale viene poi condiviso con l'OdV e successivamente sottoposto agli Organi di vertice, così come indicato al precedente punto 3.6.b).

Modifiche organizzazione

La DRC segnala tempestivamente alla DCS (i) le modifiche dell'assetto organizzativo; (ii) le modifiche alle responsabilità delle singole funzione aziendali.

La DAL e/o la DPPA e/o la DPRPA e/o la DADDB, per quanto di competenza, segnalano tempestivamente alla DCS i mutamenti del perimetro delle attività svolte dalla Società, frutto di nuova normativa e/o dettati da accordi con Amministrazioni/Enti.

La DCS, verificata la necessità di aggiornamento del Modello e/o del Codice Etico con l'OdV, avvia le attività di approfondimento e, successivamente, di redazione/integrazione con il supporto del Gruppo di lavoro, se necessario.

Il documento finale viene poi condiviso con l'OdV e successivamente sottoposto agli Organi di vertice, così come indicato al precedente punto 3.6.b).

Risk assessment integrato

In caso di:

- identificazione di nuove attività a rischio o variazione di quelle precedentemente identificate, anche eventualmente connesse all'avvio di nuove attività
- aggiornamento del risk assessement integrato

la DCS, verificata la necessità di aggiornamento del Modello e/o del Codice Etico con l'OdV, avvia le attività di redazione/integrazione con il supporto del Gruppo di lavoro, se necessario.

Il documento finale viene poi condiviso con l'OdV e successivamente sottoposto agli Organi di vertice, così come indicato al precedente punto 3.6.b).

Segnalazione ambiti di miglioramento

In caso di:

- riscontro di carenze e/o lacune nelle previsioni del Modello e/o del Codice Etico a seguito di (i) verifiche sull'efficacia del medesimo, occasionali o svolte dall'OdV; (ii) segnalazioni/verifiche svolte dal RPCT, dal DP, dal DPO, dal GSOS o dalla funzione di IA; (iii) segnalazioni provenienti da altri organi, dipendenti o da terzi; (iv) segnalazioni provenienti dalle RSU
- significative violazioni delle prescrizioni del Modello e/o del Codice Etico complessivamente inteso o del PTPC

la DCS, verificata la necessità di aggiornamento del Modello e/o del Codice Etico con l'OdV, avvia le attività di redazione/integrazione con il supporto del Gruppo di lavoro, se necessario.

Il documento finale viene poi condiviso con l'OdV e successivamente sottoposto agli Organi di vertice, così come indicato al precedente punto 3.6.b).

3.6.d) Comunicazione e pubblicazione del Modello e/o del Codice Etico

Conseguentemente alla delibera di approvazione del Modello e/o del Codice Etico da parte del CdA:

(i) il Modello e/o il Codice Etico viene pubblicato, a cura della DCS, sul sito internet della Società, all'interno della sezione Società Trasparente, sotto-sezione Livello 1 "*Disposizioni generali*"

(ii) la DCS dà comunicazione della pubblicazione Modello e/o del Codice Etico a tutto il personale della Società

Ogni nuova versione del Modello e/o del Codice Etico viene pubblicata all'interno della sezione Società Trasparente con le modalità previste nella Sezione Trasparenza del PTPC e per una durata di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione; decorso tale termine il documento rimane accessibile ai sensi dell'art. 5 del d.lgs. 33/2013 (Accesso civico).

3.7 I DESTINATARI E I REFERENTI DEL MODELLO

3.7.a) Destinatari

I destinatari delle prescrizioni del Modello e del Codice Etico, ai sensi del Decreto e, nell'ambito delle rispettive competenze, sono tenuti alla conoscenza ed osservanza delle stesse (i "Destinatari").

Sono considerati tali:

a. i componenti del Consiglio di Amministrazione, in ogni decisione o azione relativa alla gestione della Società e all'attuazione dell'oggetto sociale;

b. i componenti del Collegio Sindacale, nella vigilanza sull'osservanza della legge e dello statuto, sul rispetto dei principi di corretta amministrazione e sull'adeguatezza dell'assetto organizzativo, amministrativo, e contabile adottato dalla Società e sul suo concreto funzionamento;

c. i membri dell'OdV;

d. i dirigenti ed, in generale, i responsabili delle varie funzioni aziendali di Consip, nel dare concreta esecuzione alle attività di direzione della Società, nella gestione delle attività interne ed esterne;

e. i dipendenti e tutti i collaboratori di Consip, a qualsiasi titolo, anche occasionali e/o soltanto temporanei;

f. tutti coloro che intrattengono rapporti commerciali e/o finanziari di qualsiasi natura con la Società, ovvero agiscono per conto della stessa sulla base di specifici mandati.

3.7.b) Principi di comportamento dei Destinatari

I Destinatari - ciascuno nell'ambito delle proprie competenze e delle proprie mansioni ed incarichi svolti a qualsiasi titolo per conto di Consip - sono tenuti a rispettare rigorosamente le prescrizioni del Modello e/o del Codice Etico e, in generale, a comportarsi sempre secondo criteri di correttezza e trasparenza, nonché ad evitare comportamenti, anche omissivi, tali da impedire od ostacolare il rispetto del Modello e/o del Codice Etico ed i controlli relativi alla sua applicazione da parte dell'Organismo di Vigilanza. In particolare è fatto divieto ai Destinatari di:

a. porre in essere comportamenti costituenti condotte tipiche richiamate dal Decreto, o comunque contrarie ad una qualunque legge in vigore;

b. porre in essere comportamenti o interpretazioni non conformi al Decreto, nell'ambito della concreta applicazione dei seguenti atti o documenti:

   (i) procedure interne rilevanti ai sensi del Decreto adottate dalla Società sotto qualsiasi forma (procedure, circolari interne, ordini di servizio, linee guida ecc.);

   (ii) principi, protocolli e misure preventive individuate nel Modello;

   (iii) prescrizioni contenute nel Codice Etico.

3.7.c) Referenti

L'attuazione del Modello e del Codice Etico, che incide trasversalmente sull'intera struttura aziendale, impone l'individuazione di alcune figure all'interno della struttura stessa, che fungano da punto di riferimento con riguardo alle aree di competenza. I Referenti sono individuati nei responsabili delle Divisioni aziendali e sono coinvolti, laddove necessario, nel processo di elaborazione ed esecuzione del Modello e/o del Codice Etico. Nel seguito, a titolo meramente esemplificativo, una sintesi dei compiti:

- collaborano alla redazione/aggiornamento del Modello e/o del Codice Etico in quanto membri del gruppo di lavoro, anche tramite i *Focal Points*;
- partecipano al processo di gestione del rischio;
- forniscono suggerimenti all'OdV, segnalando eventuali criticità riscontrate, per l'aggiornamento e integrazione del Modello e/o del Codice Etico;

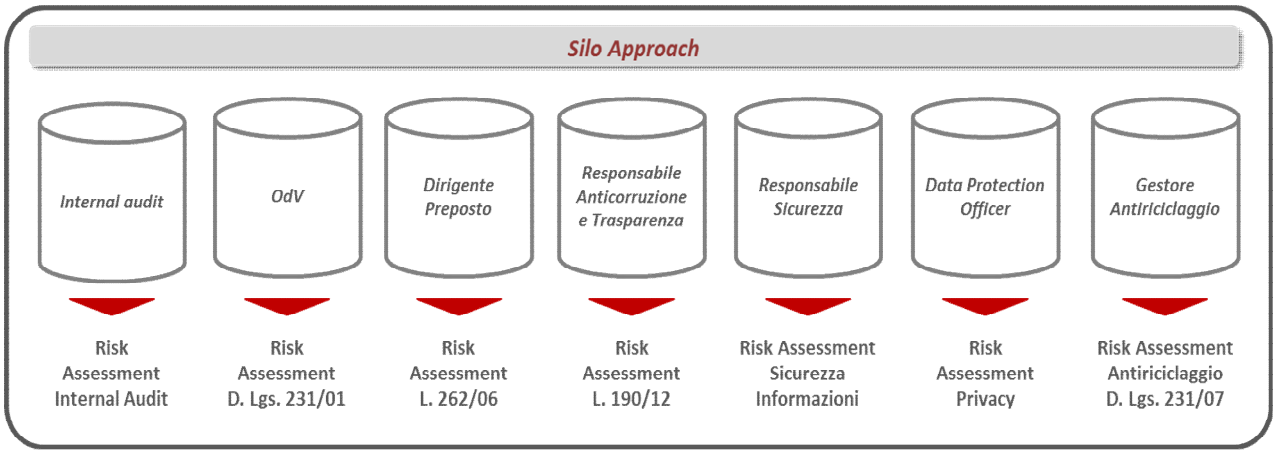
- osservano le misure contenute nel Modello e/o del Codice Etico e assicurano il rispetto dello stesso da parte delle proprie risorse;
- segnalano le situazioni di illecito a seguito di commissione di uno dei reati previsti dal Decreto;
- collaborano con l'OdV per l'esecuzione e attuazione del Modello e/o del Codice Etico e forniscono il supporto e la collaborazione necessari allo svolgimento dei propri compiti, ciascuno per la Divisione di rispettiva competenza;
- assicurano i flussi di informazioni definiti nel Modello e nelle procedure aziendali;
- trasmettono il report periodico per segnalare eventuali eventi/criticità di interesse che impattano sui centri di rischio di competenza.

Per le attività connesse all'aggiornamento/esecuzione del Modello e/o del Codice Etico, i Referenti possono individuare uno o più *Focal Points* all'interno della rispettiva struttura, con lo scopo di fornire alla DCS e all'OdV, ciascuno per le materie di rispettiva competenza, il supporto necessario e garantire, al contempo, il più ampio coinvolgimento di tutti gli uffici interessati alle tematiche trattate. E' compito dei *Focal Points* condividere con il rispettivo Referente e le strutture di appartenenza le attività svolte di volta in volta nei differenti gruppi di lavoro che si dovessero costituire, anche per l'aggiornamento del Modello e/o del Codice Etico, al fine di raccogliere e sottoporre alla DCS e all'OdV eventuali criticità o proposte migliorative.

CAPITOLO 4
GESTIONE DEL RISCHIO

4.1 RISK ASSESSMENT INTEGRATO

La Società ha effettuato alcune valutazioni sull'opportunità di adottare una differente metodologia in sostituzione di quella suggerita dal Piano Nazionale Anticorruzione ed utilizzata nel PTPC della Società o di quelle utilizzate dall'OdV e dall'IA, che consentisse una ponderazione del rischio più coerente con le attività aziendali, nonché di sfruttare la piena sinergia delle funzioni di controllo attraverso l'integrazione e la razionalizzazione dei rischi, andando ad efficientare il relativo processo. Il modello di gestione dei rischi, della *compliance* e dei controlli adottato fino al 2017 da Consip era infatti definibile come *silo approach*, dove ogni struttura, nell'ambito del proprio ambito verticale di gestione, autonomamente definiva ed applicava metodologie e strumenti di analisi dei rischi, di controllo e di reporting.



All'esito degli approfondimenti, nel corso del 2017 è stato dunque avviato il "*Progetto per lo sviluppo di metodologie integrate di analisi e valutazione dei rischi*". Tale Progetto, che inizialmente prevedeva un'analisi dei rischi integrata con riferimento al d.lgs. 231/01, alla L. 190/12 e al d.lgs. 33/2013, è stato poi esteso anche ad ulteriori aree di rischio:

- ✓ rischi di cui al d.lgs. 262/2005
- ✓ rischi antiriciclaggio ex d.lgs. 231/2007
- ✓ rischio privacy (GDPR)
- ✓ rischi sicurezza delle informazioni
- ✓ rischio ex d.lgs. 50/2016
- ✓ rischio operativo
- ✓ rischio di sicurezza fisica

L'analisi dei rischi è stata, dunque, condotta utilizzando una metodologia *risk based e process oriented,* come nel seguito schematizzato e poi analizzato nei diversi paragrafi:

Analisi dei rischi

- Analisi del contesto esterno
- Analisi del contesto interno (macro-processi – processi – procedure)
- Individuazione delle aree di rischio generali e delle aree di rischio specifiche
- Individuazione e descrizione degli eventi di rischio a cui la Società risulta potenzialmente esposta con relativi Fattori abilitanti e Conseguenze
- Identificazione, per ogni rischio, delle anomalie significative e degli indicatori di rischio
- Catalogazione dei rischi individuati in apposite «Famiglie di Rischio» e predisposizione del Registro dei rischi
- Condivisione delle risultanze con le strutture

Valutazione dei rischi

- Definizione della Metodologia di valutazione dei rischi e dei presidi
- Valutazione del grado di esposizione ai rischi
- Valorizzazione (scoring) dei rischi e dei presidi di controllo: Rischio Inerente, Presidi di Controllo e Rischio Residuo
- Valorizzazione della Rischiosità Complessiva di ciascun Processo Aziendale e di ciascuna Famiglia di Rischio

Trattamento dei rischi

- Definizione dei protocolli preventivi nelle diverse Parti speciali
- Definizione delle priorità di trattamento
- Definizione dei Piani di azione di cui al PTPC, necessari per ogni area ed evento di rischio
- Definizione del Piano Integrato dei controlli

4.2 FAMIGLIE DI RISCHIO

I rischi sono stati catalogati in n. 10 «famiglie di rischio», come nel seguito indicato:

Compliance ex d.lgs. *231*/01
Mancato rispetto dei vincoli normativi in materia di responsabilità amministrativa delle persone giuridiche

Compliance ex L. 190/2012
Mancato rispetto dei vincoli normativi in tema di prevenzione della corruzione e mala administration

Trasparenza ex d.lgs. 33/2013
Mancato rispetto dei vincoli normativi in tema di trasparenza

Privacy
Mancato rispetto dei vincoli normativi in materia di protezione dei dati personali (GDPR)

Antiriciclaggio ex d.lgs. 231/2007
Mancato rispetto dei vincoli normativi in materia di antiriciclaggio e di finanziamento del terrorismo

Compliance ex d.lgs. *262*/05
Mancato rispetto dei vincoli normativi in materia di corretta rappresentazione della situazione patrimoniale, economica e finanziaria della Società

Rischio operativo
Rischio di perdite derivanti dalla inadeguatezza o dalla disfunzione di procedure, risorse umane e sistemi interni, oppure da eventi esogeni. Tale definizione ricomprende il rischio legale

Sicurezza Fisica
Rischio di accessi non autorizzati alla sede e/o ai locali aziendali e danneggiamento o sottrazione di beni e/o informazioni

Sicurezza delle Informazioni
Rischio di compromissione della riservatezza, integrità e disponibilità delle informazioni gestite dalla Società

Compliance ex d.lgs. 50/16
Mancato rispetto dei vincoli normativi in materia di contratti pubblici relativi a lavori, servizi e forniture

4.3 INDIVIDUAZIONE DELLE AREE A RISCHIO E DEI RISCHI SPECIFICI

4.3.a) Individuazione delle aree a rischio

L'individuazione delle aree di rischio ha la finalità di consentire l'emersione delle aree, nell'ambito dell'attività della Società, che debbono essere presidiate più di altre mediante l'implementazione di misure di prevenzione.

La Società ha dunque individuato le "Aree generali", che riguardano tutte le società in quanto tali, unitamente alle c.d "Aree di rischio specifiche", che si differenziano per la loro presenza in relazione alle caratteristiche dell'ente. Ad ogni Area di rischio sono stati poi ricondotti i vari processi aziendali.

L'individuazione delle aree di rischio è stata, dunque, effettuata attraverso:

- ✓ l'esame della struttura organizzativa, dei ruoli e delle responsabilità interne
- ✓ l'analisi della mappatura dei processi di funzionamento aziendali e delle procedure aziendali
- ✓ l'analisi dell'altra documentazione interna utile, costituita dai documenti organizzativi e gestionali, dal sistema di procure, ecc.
- ✓ le interviste con i *Focal Points*/Referenti, finalizzate alla rilevazione delle attività aziendali maggiormente esposte a rischio; l'analisi è stata svolta anche attraverso le indicazioni dei dirigenti/dipendenti, quale ulteriore esplicazione della loro responsabilità nell'ambito del processo di analisi dei rischi
- ✓ la condivisione con i *Focal Points*/Referenti intervistati delle risultanze dell'analisi dei rischi condotta
- ✓ il coinvolgimento dei *Focal Points*/Referenti interessati per l'individuazione e la valutazione delle misure preventive e dei Piani di azione del PTPC da adottare

4.3.b) Identificazione dei rischi

Una volta definite le Aree di rischio in base a quanto sopra rappresentato, si è proceduto ad individuare i singoli rischi ivi configurabili, elencati nel Registro dei rischi. Per ciascun rischio è stata compilata, a seconda del processo/fase, la "*Scheda di analisi del rischio*", in cui sono riportati:

- *risk owner*;
- identificazione e descrizione dei rischi che caratterizzano i macro-processi, processi e fasi elementari;
- identificazione, per ogni rischio, dei Fattori abilitanti e delle Conseguenze, nell'ottica di fornire una rappresentazione esemplificativa di tali elementi, seppur non tassativa
- identificazione, per ogni rischio, delle anomalie significative e degli indicatori di rischio;
- identificazione, per ogni rischio, delle Misure Generali e Specifiche;
- Valorizzazione dei rischi e dei presidi di controllo: Rischio Inerente, Presidi di Controllo e Rischio Residuo
- Valorizzazione della Rischiosità Complessiva di ciascun Processo Aziendale e di ciascuna

Famiglia di Rischio

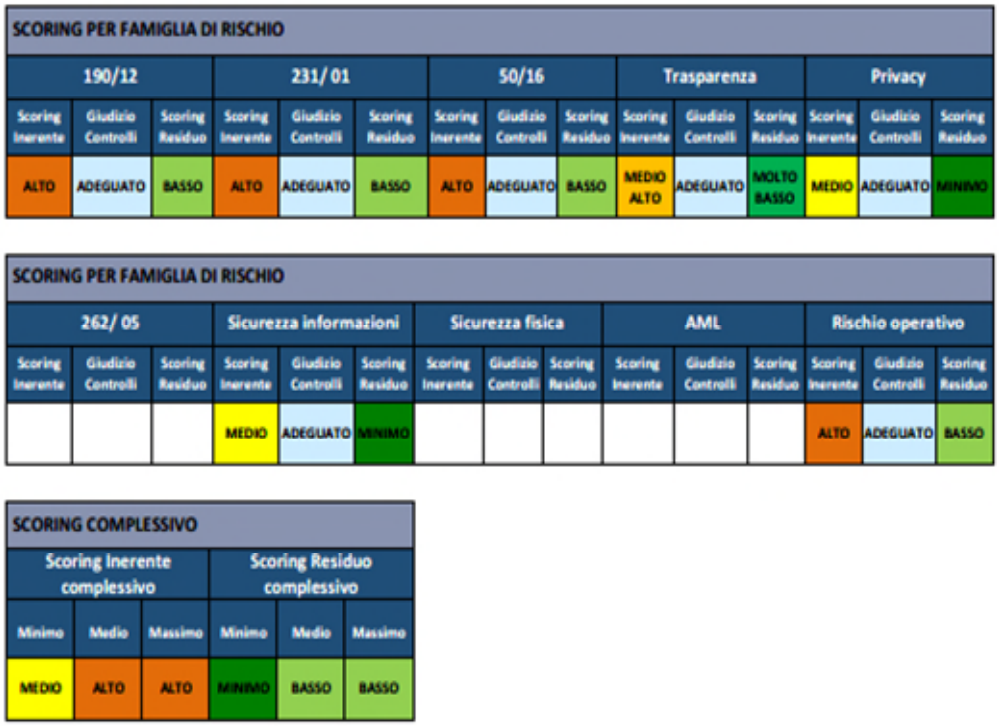
- Piani di azione di cui al PTPC suggeriti, con l'indicazione del Responsabile, della tempistica di attuazione e dell'indicatore di monitoraggio.

Scheda di analisi del rischio

R.10a

ANAGRAFICA EVENTO RISCHIO						
Codice rischio	**10a**	**Attività**	**Redazione e approvazione strategia/ Consultazione mercato - svolgimento**	**Descrizione rischio**	Non corretto svolgimento della consultazione del mercato al fine di favorire un'impresa o un gruppo di imprese/favorire la Società attraverso: – alterazione del campione di imprese consultato; – non corretto utilizzo degli incontri con i fornitori.	
Risk-owner	→ Sourcing-CM		**Contributor**	– Sourcing-ALS	**Macro-Processo**	Sviluppo Iniziative di Acquisto
					Processo	Sviluppo Convenzione/ Accordo quadro/ Contratto quadro
					Fase	Strategia
Area	Generale Affidamento di lavori, servizi e forniture			**Sotto Area**	Generale Definizione dell'oggetto dell'affidamento	
DETTAGLIO RISCHIO						
Fattori abilitanti	✓ Scarsa procedimentalizzazione del processo ✓ Esercizio prolungato ed esclusivo di responsabilità di una fase da parte di uno o pochi soggetti ✓ Errore operativo ✓ Accordi illeciti ✓ Mancato rispetto delle regole procedurali interne ✓ Mancato/ errato recepimento della normativa di settore ✓ Assenza controlli			**Conseguenze**	✓ perdita economica ✓ danno erariale ✓ sanzioni ✓ inefficienza ✓ danno reputazionale	
Riferimenti normativa esterna	• L. n. 190/2012 • D.Lgs. n. 33/2013 • D.Lgs. n. 231/2001 • D.Lgs. n. 50/2016 • Linee Guida ANAC n. 14		**Riferimenti normativa interna**		o Attività e responsabilità del processo di acquisizione di beni e servizi sopra soglia - fase strategia o Modalità Operative per la consultazione del mercato o Standard questionario generale e tecnico o Procedura e Policy per la tenuta e aggiornamento del Registro delle persone che hanno accesso alle Informazioni Privilegiate o Linee Guida Gestione Conflitto di Interessi o Politica per la classificazione delle informazioni o Procedura per la gestione degli aspetti di sicurezza nel ciclo di vita delle Informazioni	
Anomalie significative	Presenza di gare aggiudicate con frequenza agli stessi soggetti per la medesima merceologia		**KRI**	0 / 2	**Indicatori di rischio**	0) Segnalazioni pervenute 2a) procedure aggiudicate allo stesso fornitore per la medesima merceologia (con riguardo all'ultimo triennio/ultime tre edizioni della stessa iniziativa) 2b) ricorsi aventi ad oggetto l'erronea definizione dell'impianto di gara

CONTROLLI	
Sintesi misure di controllo	
✓ Politiche di gestione del rischio (MOG/PTPC/CE) ✓ Politiche di Gestione del rischio privacy ✓ Trasparenza ✓ Segregazione compiti/funzioni ✓ Controlli gerarchici ✓ Audit/ Controlli ✓ Sistema deleghe/procure ✓ Tracciabilità del processo ✓ Archiviazione documentazione rilevante ✓ Rotazione ✓ Reporting	✓ Flussi informativi ✓ Informatizzazione processo ✓ Gestione conflitto interessi ✓ Gestione riservatezza informazioni ✓ Formazione ✓ Whistleblowing ✓ Certificazioni ✓ Sistema disciplinare ✓ Sistema procedurale interno ✓ Accesso civico
Misure generali	**Misure specifiche**
La Società si è dotata: – PTPC, Codice etico e Modello ex D.Lgs. 231/2001 – Specifiche regole a garanzia della riservatezza delle informazioni – Sistema disciplinare interno finalizzato a sanzionare il mancato rispetto del sistema procedurale interno e dei principi contenuti nel PTPC, del Codice etico e del Modello ex D.Lgs. 231/2001 – Regolamento per la gestione dell'accesso civico semplice e generalizzato – Linee guida conflitto interessi – Piano Integrato dei Controlli – Sistema di whistleblowing – Flussi informativi vs organi di controllo sia periodici che ad evento – Piano integrato di Formazione (d.lgs 231/2001, L. 190/12, d.lgs. 231/07 e GDPR) – Piano Pluriennale di rotazione	– La società si è dotata di una procedura interna volta a disciplinare le modalità di espletamento e pubblicità della consultazione del mercato, che impone l'obbligo di individuare criteri oggettivi per la selezione dei fornitori da incontrare, elaborata nel rispetto della segregazione dei compiti e delle funzioni - per ciascuna fase sono individuati (i) i ruoli e le responsabilità di tutti i soggetti coinvolti; (ii) i controlli gerarchici per la definizione delle modalità della consultazione/criteri, sia da parte del responsabile di Area che del responsabile di Divisione – Condivisione delle logiche e dei criteri della consultazione tra Sourcing - CM e ALS – Pubblicazione, nella sezione "società trasparente – bandi di gara e contratti" del sito internet Consip, del Documento di consultazione del mercato preventivamente condiviso con i responsabili gerarchici (responsabile di area Sourcing e responsabile di Divisione Sourcing) – Prevista pubblicazione di un questionario generale e invio di un questionario tecnico ai fornitori che hanno risposto, che vengono poi conservati nella documentazione inerente l'iniziativa – In alcuni casi (mercato fornitura molto esteso) individuazione di campionamento con criteri oggettivi, esplicitati nel documento di consultazione – Le interviste agli operatori economici sono effettuate alla presenza di almeno due dipendenti Consip –dell'incontro viene redatto apposito verbale, sottoscritto da tutti i partecipanti – La sintesi della consultazione viene elaborata dal CM con il supporto del referente legale, e riportata nella strategia Reporting periodico sulle consultazioni di mercato da Ad a CdA/CS – La Società si è dotata di un Registro dei soggetti che detengono e/o hanno accesso alle informazioni relative alle procedure di gara e policy interna – Il processo è certificato: Certificazione ISO 9001:2015
PIANI D'AZIONE SUGGERITI	
//	



SCORING PER FAMIGLIA DI RISCHIO															
190/12			231/01			50/16			Trasparenza			Privacy		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
ALTO	ADEGUATO	BASSO	ALTO	ADEGUATO	BASSO	ALTO	ADEGUATO	BASSO	MEDIO ALTO	ADEGUATO	MOLTO BASSO	MEDIO	ADEGUATO	MINIMO

SCORING PER FAMIGLIA DI RISCHIO														
262/05			Sicurezza informazioni			Sicurezza fisica			AML			Rischio operativo		
Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo	Scoring Inerente	Giudizio Controlli	Scoring Residuo
			MEDIO	ADEGUATO	MINIMO							ALTO	ADEGUATO	BASSO

SCORING COMPLESSIVO					
Scoring Inerente complessivo			Scoring Residuo complessivo		
Minimo	Medio	Massimo	Minimo	Medio	Massimo
MEDIO	ALTO	ALTO	MINIMO	BASSO	BASSO

Ogni scheda rischio è stata poi condivisa con i rispettivi Referenti e focal point.

Le risultanze complessive sono sintetizzate nei seguenti documenti:

- Matrice "Rischi Reato/Referenti" contenente l'elenco dei reati presupposto che, a livello teorico, è possibile siano commessi dai Destinatari con indicazione dei relativi Referenti aziendali responsabili dell'attività a rischio e, dunque, dell'effettiva applicazione dei presidi di controllo posti in essere;

- Matrice delle Attività Rischio Reato contenente la mappatura delle aree a rischio, associate alle fattispecie di reato con esempi di possibili modalità di realizzazione dei reati e dei macro processi strumentali/funzionali potenzialmente associabili, unitamente all'identificazione delle Parti Speciali del Modello a cui sono associate le rispettive attività a rischio.

La DCS gestisce, inoltre, uno specifico Registro dei rischi contenente l'elenco degli eventi di rischio individuati, distinti per processo/fase/attività; tale documento favorisce la registrazione, gestione e monitoraggio dei rischi e delle azioni di mitigazione. E' in fase di elaborazione il tool informatico per la gestione del Registro.

4.5 VALUTAZIONE DEI RISCHI

Come sopra già accennato, per ciascun rischio mappato, nell'ambito delle relative Famiglie di Rischio, sono stati valorizzati:

Rischio Inerente	possibilità che nello svolgimento di una attività si verifichi un evento dannoso in assenza di controlli (impatto massimo di una data attività)
Misure Esistenti	presenza o meno di uno o più dei seguenti presidi di controllo: - Politiche di gestione del rischio (MOG/PTPC/CE) - Politiche di gestione del rischio privacy - Politiche di gestione del rischio antiriciclaggio - Politiche di gestione ex L. 262/05 - Trasparenza - Segregazione compiti/funzioni - Controlli gerarchici - Controlli/Audit - Sistema deleghe/procure - Tracciabilità del processo - Archiviazione documentazione rilevante - Rotazione - Reporting - Flussi informativi - Informatizzazione processo - Gestione conflitto interessi - Gestione incompatibilità - Gestione riservatezza informazioni - Formazione - Whistleblowing - Certificazioni - Sistema disciplinare - Sistema procedurale interno - Accesso civico - Disciplina revolving doors - Accordi/contratti
Rischio Residuo	possibilità che si verifichi un evento dannoso dopo l'implementazione dei controlli

Per ogni misura preventiva esistente, sono indicate, nel paragrafo 4.7, la definizione ed i contenuti specifici.

4.5.a) Metodologia di Valutazione del Rischio Inerente

Il rischio inerente è stato valorizzato assegnando ad ogni rischio individuato un *risk scoring* basato sulla valutazione correlata di due parametri:

- ➔ probabilità di accadimento
- ➔ impatto

sulla base di quanto indicato nelle matrici che seguono

Matrice di valutazione della probabilità

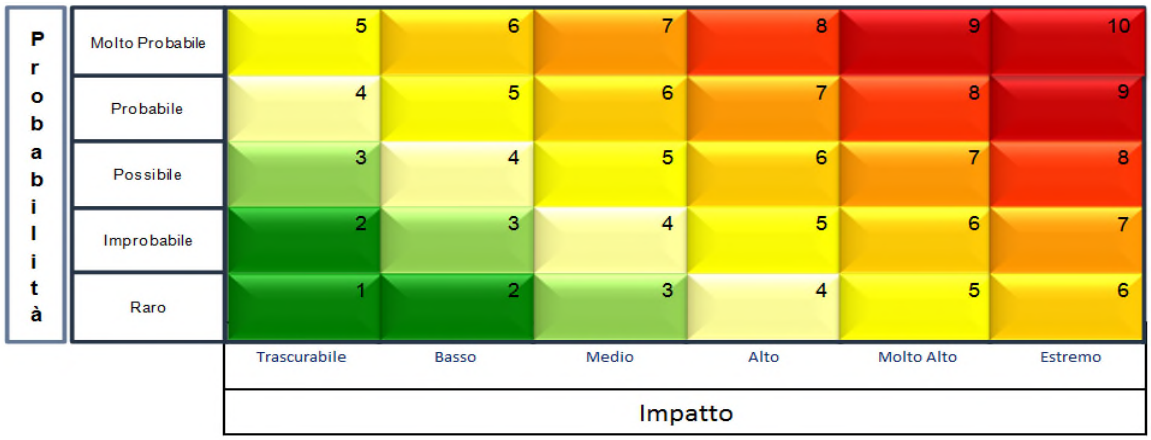
CATEGORIE	FATTORI
Molto probabile	•>75% probabilità, o •l'evento si è verificato negli ultimi mesi
Probabile	•<75% probabilità, o •l'evento si è verificato negli ultimi 12 mesi
Possibile	•<50% probabilità, o •l'evento si è verificato negli ultimi tre anni
Improbabile	•<25% probabilità, o •l'evento si è verificato negli ultimi cinque anni
Raro	•<1% probabilità, o •l'evento non si è mai verificato nel passato o si è verificato una sola vota negli ultimi dieci anni

Matrice di valutazione dell'impatto

		CATEGORIE					
		Trascurabile	**Basso**	**Medio**	**Alto**	**Molto Alto**	**Estremo**
FATTORI	**Descrizione Categorie**	Impatto trascurabile sul raggiungimento degli obiettivi di processo.	Impatto basso sul raggiungimento degli obiettivi di processo.	Impatto moderato su uno o più obiettivi di processo.	Impatto rilevante su uno o più obiettivi di processo.	Elevato impatto sul raggiungimento degli obiettivi di processo	Pregiudizio alla continuità del business.
				Moderate inefficienze	Consistenti inefficienze		Elevato impatto sul raggiungimento degli obiettivi di processo "strategici".
				Moderata inefficacia di alcuni processi	Non sporadica inefficacia di alcuni processi		Elevato impatto su molteplici processi aziendali.
	Variazione negativa EBIT	x< 1% ovvero	1%<x<3% ovvero	3%<x<,5,8% ovvero	5,8%<x<8% ovvero	8%<x<10% ovvero	x>10% ovvero
	Sicurezza delle informazioni	Perdita di riservatezza di dati non rilevanti (Informazioni classificate "**Public**")	Perdita di riservatezza di dati rilevanti di natura non strategica senza implicazioni sul business e sulla compliance (Informazioni classificate "**Internal**")	Perdita di riservatezza di dati rilevanti di natura non strategica con parziali implicazioni sul business e non sulla compliance (Informazioni classificate "**Internal**")	Perdita di riservatezza di dati rilevanti di natura non strategica con implicazioni sul business e non sulla compliance (Informazioni classificate "**Internal**" o "**Confidential**")	Perdita di riservatezza di dati rilevanti di natura non strategica con implicazioni sul business e sulla compliance (Informazioni classificate "**Confidential**")	Perdita di riservatezza di dati rilevanti di natura strategica con implicazioni sul business e sulla compliance (Informazioni classificate "**Confidential**")
		Perdita di disp./int. di informazioni che non sono bloccanti per il processo. Le informazioni non hanno un impatto sul business e la perdita di disponibilità può essere facilmente gestibile	Perdita di disp./int. di informazioni che non sono bloccanti per il processo. Le informazioni non hanno un impatto sul business e la perdita di disponibilità è difficilmente gestibile	Perdita di disp./int. di informazioni che sono bloccanti per il processo. Le informazioni hanno un impatto parziale sul business.	Perdita di disp./int. di informazioni che sono bloccanti per il processo. Le informazioni hanno un impatto diretto sul business	Perdita di disponibilità di dati che sono bloccanti per il processo. Le informazioni hanno un impatto diretto sul business e / o sulla compliance	Perdita di disponibilità di dati che sono bloccanti per il processo. Le informazioni hanno un impatto critico sul business e / o sulla compliance

	Regolatorio e Compliance	Osservazioni / Ammonimenti da parte delle Authority	Sanzioni occasionali di lieve rilevanza da parte delle Authority	Sanzioni frequenti di lieve rilevanza da parte delle Authority	Sanzioni frequenti di seria rilevanza da parte delle Authority	Restrizioni dell'attività	Interruzione dell'attività
	Immagine e Reputazione	Notizie sui media locali di settore	Notizie sui media locali (di settore e non)	Notizie su media locali con esposizione mediatica di breve periodo	Notizie su media nazionali con esposizione mediatica di breve periodo	Notizie su media nazionali con esposizione mediatica di medio-lungo periodo e/o su media internazionali con esposizione mediatica di breve periodo	Notizie su media nazionali e internazionali con forte esposizione mediatica di lungo periodo

Lo *scoring* attribuito a ogni rischio deriva dall'incrocio delle valutazioni attribuite a Impatto e Probabilità di accadimento nella matrice di seguito rappresentata



Successivamente lo scoring numerico viene tradotto in classi di giudizio sulla base della sottostante tabella di transcodifica

Classi									
Minimo	**Molto Basso**	**Basso**	**Medio Basso**	**Medio**	**Medio Alto**	**Alto**	**Molto Alto**	**Massimo**	**Estremo**
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Valori									

4.5.b) Metodologia di Valutazione Presidi di Controllo

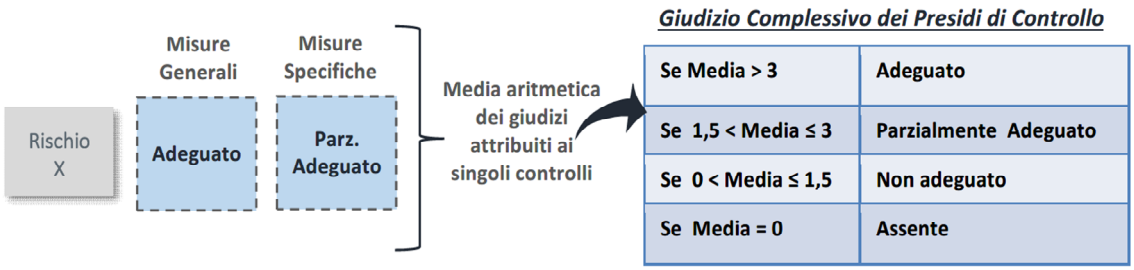
Per la valutazione dei controlli è stata considerata l'adeguatezza delle misure esistenti ovvero di tutti gli strumenti, le azioni ed i presidi che possono contribuire a ridurre la probabilità del compimento (verificarsi di reati presupposto/pratiche di corruzione o a contenerne l'impatto, distinguendole in:

misure generali	Quelle che intervengono in maniera trasversale sull'intera amministrazione e si caratterizzano per la loro incidenza sul sistema complessivo della prevenzione dei rischi
misure specifiche	Quelle che agiscono in maniera puntuale su alcuni specifici rischi individuati in fase di valutazione del rischio e si caratterizzano, dunque, per l'incidenza su problemi specifici

Ad ogni presidio di controllo è stato attribuito un giudizio di adeguatezza, considerando l'efficacia e l'efficienza dello stesso a governare i rischi individuati:

GIUDIZIO	*SIGNIFICATO*	*VALORE*
adeguato	esistente e che assicura un governo del rischio efficace ed efficiente	4
parzialmente adeguato	esistente e che assicura un governo del rischio parziale in termini di efficacia ed efficienza	2
non adeguato	esistente ma non adeguato ad assicurare il governo del rischio	1
assente	non esistente	0
n.a.	non applicabile	-

Per ogni rischio sono stati quindi valorizzati i Presidi di Controllo – Misure Generali e Misure Specifiche - e calcolato il «Giudizio Complessivo dei Presidi di Controllo» ottenuto dalla media aritmetica dei giudizi attribuiti a ciascuno di essi. Il Giudizio è stato quindi valorizzato sulla base degli algoritmi di seguito riportati:

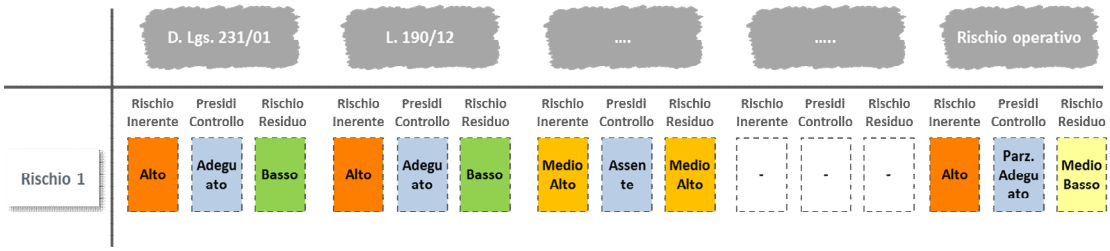


4.5.c) Metodologia Valutazione Rischio Residuo

Il risk scoring Residuo è stato calcolato come differenza tra il Valore associato al Rischio Inerente e il Valore associato ai Presidi di controllo

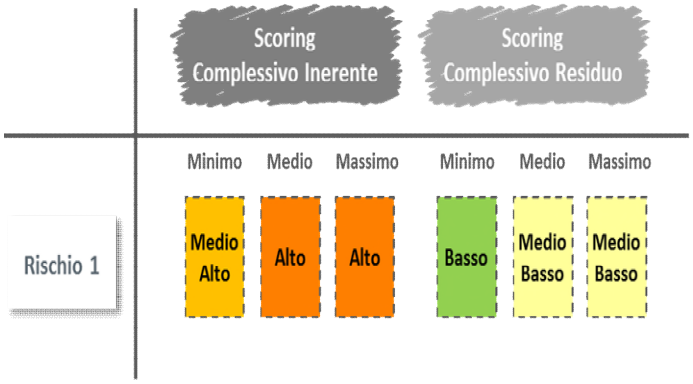
rischio inerente – presidi di controllo = rischio residuo

Per ogni evento di rischio, nell'ambito di ciascuna famiglia di rischio a cui esso è associato, sono stati poi valutati il Rischio Inerente, i Presidi di Controllo e conseguentemente il Rischio Residuo, come nel seguito esemplificato:



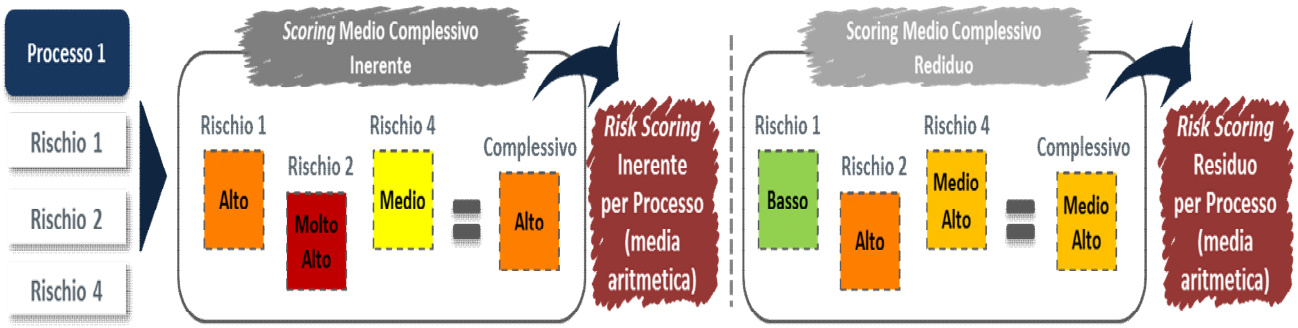
4.5.d) Rischiosità complessiva media e per processo

Per ciascun evento di rischio sono stati individuati i tre Risk Scoring: minimo, medio e massimo assunti complessivamente su base inerente e residua:



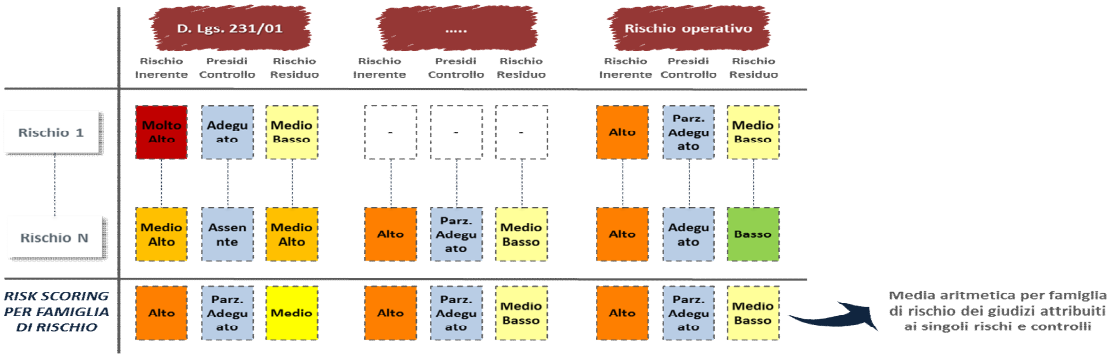
- Lo *scoring* complessivo minimo corrisponde allo *scoring* minimo assunto complessivamente da un dato evento di rischio nell'ambito di tutte le Famiglie di Rischio nelle quali risulta valorizzato
- Lo *scoring* complessivo medio corrisponde alla media degli *scoring* assunti da un dato evento di rischio nell'ambito di tutte le Famiglie di Rischio nelle quali risulta valorizzato
- Lo *scoring* complessivo massimo corrisponde allo *scoring* massimo assunto complessivamente da un dato evento di rischio nell'ambito di tutte le Famiglie di Rischio nelle quali risulta valorizzato

La rischiosità complessiva inerente e residua per Processo corrisponde, dunque, alla media dei Risk Scoring Medi Complessivi assunti da ciascun evento di rischio presente su tale processo.



4.5.e) Rischiosità complessiva per Famiglia di Rischio

La rischiosità inerente e residua per «famiglia di rischio» è calcolata come media degli *scoring* attribuiti ai singoli eventi di rischio presenti nella Famiglia stessa.



4.5.f) Fattori abilitanti, conseguenze, anomalie significative e indicatori di rischio

Gli indicatori di rischio sono strumenti utilizzabili dalle organizzazioni per l'individuazione tempestiva di segnali preventivi (*red flags*) in caso di emersione di un nuovo rischio oppure di aumento dell'esposizione ad un rischio già presente in diverse aree di attività. L'emersione di uno o più *red flags* può generare l'effettuazione di interventi correttivi, come ad esempio specifiche attività di controllo.

In ottemperanza a quanto definito da ANAC con il PNA 2015, il PNA 2016 e il PNA 2019, ogni scheda di rischio riporta - ove possibile - l'indicazione dei fattori abilitanti degli eventi rischiosi, delle conseguenze, delle anomalie significative e degli indicatori di rischio corruzione.

Periodicamente i dati raccolti a tale scopo vengono dunque analizzati con il supporto della Divisone Internal Audit e della Divisione Compliance e Societario, al fine di

- ✓ verificare l'efficacia e la significatività degli indicatori di rischio individuati;
- ✓ definire le esigenze in termini di controllo, conseguenti le risultanze dell'analisi di cui sopra, da far poi confluire nel Piano Integrato dei Controlli;
- ✓ apportare agli indicatori le eventuali modifiche/integrazioni necessarie, eventualmente coinvolgendo i Focal Points/Referenti interessati.

4.6 TRATTAMENTO DEI RISCHI

Il trattamento dei rischi riguarda la definizione delle strategie di risposta al rischio e l'individuazione di azioni specifiche da implementare al fine di allineare il profilo di rischio attuale al livello di rischio considerato accettabile, in maniera tale da impedire o limitare il compimento di pratiche corruttive.

Nel sistema di trattamento del rischio sono ricomprese le azioni che contribuiscono a ridurre la probabilità di manifestazione dei reati presupposto. Il sistema di trattamento dei rischi e concepito dalla Società è costituito da molteplici elementi che in sintesi possono così riepilogarsi:

- ✓ disposizioni di carattere generale che riguardano la Società e la sua organizzazione nel complesso e che contribuiscono a ridurre la probabilità di commissione di comportamenti corruttivi (c.d. Misure Generali)

- ✓ disposizioni specifiche che riguardano i singoli ambiti a rischio e che sono finalizzati a definire il sistema di trattamento del rischio specifico per ciascun processo (c.d. Misure Specifiche)
- ✓ tempi di attuazione delle predette disposizioni
- ✓ soggetti responsabili dell'attuazione delle predette disposizioni
- ✓ indicatori di monitoraggio

La descrizione delle disposizioni di carattere generale e specifiche è contenuta nelle singole Schede di analisi del rischio nella sezione "Piani di azione suggeriti". Nel Registro dei rischi sono tracciati, per ogni Piano di azione:

- ✓ i responsabili dell'attuazione del singolo Piano di azione;
- ✓ gli output;
- ✓ le tempistiche massime.

Il RPCT monitora il rispetto dei tempi e l'effettiva implementazione dei predetti Piani di azione, anche ai fini dell'aggiornamento del profilo di rischio residuo rispetto a quello considerato accettabile, in considerazione dei miglioramenti implementati dalla Società; le risultanze del monitoraggio dei Piani di azione sono riportate nel PTPC e nelle relazioni del RPCT, trasmesse anche all'OdV. Le attività di monitoraggio di cui sopra vanno dunque ad integrare il complesso sistema dei controlli della Società ed, in particolare, il Piano Integrato dei Controlli (PIC), così come descritto nella sezione dedicata del presente Modello.

4.7 MISURE PREVENTIVE DI CONTROLLO DEL RISCHIO GENERALI

Per misure preventive si intendono tutti gli strumenti, le azioni ed i presidi che possono contribuire a ridurre la probabilità di compimento di reati presupposto/verificarsi di pratiche di corruzione o a contenerne l'impatto.

Tra queste, le misure preventive "generali" intervengono in maniera trasversale sull'intera struttura societaria e si caratterizzano per la loro incidenza sul sistema complessivo della prevenzione. Si descrivono di seguito le principali misure preventive aventi carattere generale, già adottate dalla Società, cui si devono ispirare le procedure interne.

- ✓ Politiche di gestione del rischio (MOG/PTPC/CE):
  - il Modello di Organizzazione, Gestione e controllo ex d. lgs. 231/2001 = documento che individua una serie di protocolli preventivi, finalizzati a far fronte al rischio di commissione di reati presupposto commessi nell'interesse o a vantaggio della Società. Il Modello rappresenta, dunque, un sistema strutturato ed organico di processi, procedure ed attività di controllo (preventivo ed *ex post*), che coinvolge ogni aspetto dell'attività della Società.
  - Il Piano triennale per la prevenzione della corruzione e della trasparenza ex L. 190/2012 e d. Lgs. 33/2013 = strumento per l'individuazione di misure concrete, da realizzare con certezza e da monitorare quanto ad effettiva applicazione ed efficacia preventiva della

corruzione. Esso definisce obblighi e misure, ivi inclusi quelli in tema di trasparenza, che coinvolgono l'intera struttura aziendale nella prevenzione della corruzione, sebbene a livelli e con modalità differenti. La Legge 190/2012 fa riferimento ad un concetto ampio di corruzione, in cui rilevano non solo l'intera gamma dei reati contro la P.A. disciplinati dal Titolo II del Libro II del codice penale, ma anche le situazioni di "cattiva amministrazione" *("maladministration")*.

- Il Codice Etico = inteso come codice contenente i principi di "deontologia aziendale" che la Società riconosce come propri e dei quali richiama l'osservanza da parte di tutti i destinatari del documento predetto.

✓ **Politiche gestione 262:** strumenti adottati per garantire il rispetto dei vincoli normativi di cui alla L. 262/2005 "Disposizioni per la tutela del risparmio e la disciplina dei mercati finanziari") in materia di corretta rappresentazione della situazione patrimoniale, economica e finanziaria della Società.
Include la definizione di procedure amministrative e contabili per la formazione del bilancio di esercizio ed i controlli effettuati dal Dirigente preposto ai sensi della L. 262/2005.

✓ **Politiche gestione Privacy** (ex Regolamento UE/2016/679 – GDPR e d. Lgs 196/2003)**:** strumenti adottati per garantire il pieno rispetto dei vincoli normativi in materia di tutela dei dati personali. Include:

- le procedure del Sistema privacy;
- le Istruzioni Operative per il trattamento dei dati personali;
- la nomina del Data Protection Officer (DPO).

✓ **Politiche gestione antiriciclaggio** (ex d.lgs. 231/2007)**:** strumenti adottati per garantire il pieno rispetto dei vincoli normativi in materia di antiriciclaggio e di contrasto al finanziamento del terrorismo, delineando così un sistema di prevenzione dei rischi connessi con il riciclaggio ed il finanziamento del terrorismo. Include:

- il Modello Antiriciclaggio, approvato dal CdA;
- la nomina del Gestore delle segnalazioni di operazioni sospette in materia di riciclaggio e finanziamento del terrorismo.

✓ **Segregazione dei compiti/funzioni**: distinzione delle competenze finalizzata alla suddivisione delle attività di un dato processo aziendale tra più utenti e funzioni diverse. La segregazione è sostanzialmente applicata attraverso l'adeguata separazione dei poteri e delle responsabilità fra le diverse funzioni aziendali e, soprattutto, attraverso il coinvolgimento nei vari processi di distinti soggetti muniti di diversi poteri/responsabilità, affinché nessuno possa disporre di poteri illimitati e svincolati dalla verifica altrui.

✓ **Controlli gerarchici:** controlli permanenti di I livello svolti direttamente dai responsabili gerarchici (Responsabili Area/Responsabili Divisione) e descritti nelle singole procedure aziendali.

- ✓ Audit/Controlli: sono inclusi
  - controlli permanenti di II livello effettuati da organi di II livello (RPCT; OIV; DP; Compliance; DPO; GSOS; Qualità).
  - controlli periodici di III livello effettuati da organo di III livello (Divisione Internal Audit);
  - controlli effettuati dagli organi societari di governo e controllo (CdA; CS; Magistrato della Corte dei Conti; OdV; Società di revisione legale).

- ✓ Sistema deleghe/procure: sistema adottato dalla Consip; ripercorre il quadro che emerge dall'Organigramma aziendale, sovrapponendosi ed integrandosi allo stesso. Include:
  - procure conferite da AD a Responsabili di Divisione (per compimento di atti esterni);
  - deleghe/procure conferite da Responsabili di Divisione a proprie risorse (per compimento atti interni/esterni).

  Il sistema di deleghe/procure prevede un sistema di reportistica.

- ✓ Tracciabilità del processo: raccolta ordinata di informazioni/atti/azioni che consentono di documentare l'iter/processo seguito.

- ✓ Archiviazione documentazione rilevante: conservazione di documentazione/dati su supporto cartaceo ed informatico.

- ✓ Rotazione: spostamento di una risorsa su altre attività o in altra area/divisione.
  Include:
  - Programma pluriennale di rotazione degli incarichi riguardante le aree maggiormente esposte al rischio corruzione, adottato dalla Società;
  - Rotazione per cause di incompatibilità/conflitto di interessi; in base a quanto definito nel Codice etico della società, ogni dipendente ha l'obbligo di segnalare eventuali cause di conflitto di interessi/incompatibilità che dovessero insorgere con riguardo alle attività svolte.
  - Rotazione straordinaria in caso di avvio di procedimenti penali o disciplinari per condotte di natura corruttiva; nei casi di avvio di procedimenti penali o disciplinari per condotte contestate di natura corruttiva collegate al ruolo ricoperto all'interno della Società, la stessa valuta se disporre, in via meramente cautelativa, la rotazione dell'interessato, sia dirigente che non dirigente, assegnandolo ad altro ufficio o conferendogli un altro incarico.
  - Rotazione in caso di rinvio a giudizio (art. 3 L. 97/2001); nei casi di rinvio a giudizio per i delitti richiamati dall'articolo 3, comma 1, della legge n. 97/2001 la Società dispone, in via meramente cautelativa, la rotazione dell'interessato sia dirigente che non dirigente, assegnandolo ad altro ufficio diverso da quello in cui prestava servizio al momento del fatto, con attribuzione di funzioni corrispondenti, per inquadramento, mansioni e prospettive di carriera, a quelle svolte in precedenza (laddove il delitto incida sull'attività da questi gestita).

- Rotazione per cause di inconferibilità ex d.lgs. 39/2013; in caso di sussistenza di una causa di inconferibilità, temporanea o permanente, di cui al d.lgs. 39/2013, a carico di un Dirigente, la Società opera con le modalità di cui all'art. 3 del d.lgs. 39/2013.
- Rotazione per turnover; in caso di uscita di un dipendente/dirigente, laddove possibile in base al numero di risorse disponibili ed alle competenze specifiche necessarie, la Società effettua, in via prioritaria, la rotazione del personale ai fini della copertura della posizione, anche mutando l'inquadramento del dipendente.

La Società ha inoltre adottato una tipologia specifica di rotazione:

- Rotazione dell'incarico; la Società effettua la rotazione del personale con riguardo al conferimento di specifici incarichi (Presidente della commissione di gara; membro della commissione di gara; Direttore dell'esecuzione; Responsabile del procedimento) nel rispetto della normativa vigente in materia di acquisizione di beni, servizi e forniture, in base ai criteri espressamente indicati nelle procedure aziendali di riferimento.

✓ **Reporting:** report periodico specificatamente previsto da procedure interne e/o norme di legge.

✓ **Flussi informativi:**

Include

- report periodico nei confronti di RPCT/OdV/DPO/GSOS, a carico dei Referenti anticorruzione e trasparenza, con lo scopo di ragguagliare con cadenza periodica gli organi di controllo sulle attività di competenza aventi rilevanza ex L. 190/12, d.lgs. 231/01, GDPR e d.lgs. 231/07;
- flussi ad evento, come indicato nelle procedure.

✓ **Sistema gestione conflitto di interessi:** strumenti adottati dalla Società per la gestione del tema "conflitto di interessi".

Include:

- Linee guida sul conflitto di interessi:
- Registro dei conflitti di interesse;
- dichiarazioni rese da singoli soggetti nelle varie fasi dei processi (dipendenti; membri del CdA; membri del CS; consulenti/collaboratori; membri commissione di gara; segretario di commissione; RdP; membri commissione collaudo; consulente qualità; DdE).

Sono inoltre previsti strumenti specifici:

- cause di incompatibilità ed inconferibilità di cui al D. Lgs. n.39/2013;
- Registro PEP "Persone politicamente esposte" al fine di tracciare le assunzioni/consulenze affidate a soggetti pubblici appartenenti a pubbliche amministrazioni "sensibili" rispetto alle attività svolte da Consip;
- black period.

✓ **Gestione incompatibilità/inconferibilità**: include gli strumenti per la gestione dei casi di incompatibilità ed inconferibilità di cui al d.lgs. 39/2013 (per incompatibilità s'intende

"l'obbligo per il soggetto cui viene conferito l'incarico di scegliere, a pena di decadenza, entro il termine perentorio di 15 giorni, tra la permanenza nell'incarico e l'assunzione e lo svolgimento di incarichi e cariche in enti di diritto privato regolati o finanziati dalla pubblica amministrazione che conferisce l'incarico, lo svolgimento di attività professionali ovvero l'assunzione della carica di componente di organi di indirizzo politico". Per inconferibilità s'intende *"la preclusione, permanente o temporanea, a conferire gli incarichi previsti dal presente decreto a coloro che abbiano riportato* condanne *penali per i reati previsti dal capo I del titolo II del libro secondo del codice penale, a coloro che abbiano svolto incarichi o ricoperto cariche in enti di diritto privato regolati o finanziati da pubbliche amministrazioni o svolto attività professionali a favore di questi ultimi, a coloro che siano stati componenti di organi di indirizzo politico"*).

La procedura da seguire per i rilievi e controlli sulla sussistenza o meno delle cause di incompatibilità e di inconferibilità è allo stato contenuta nel PTPC.

- ✓ Gestione riservatezza informazioni: misure volte a garantire la riservatezza delle informazioni e dei dati, anche personali, oggetto di trattamento

  Include:
  - protocolli specifici presenti nel MOG e nel PTPC;
  - specifici obblighi previsti nel Codice Etico;
  - disposizioni specifiche sul rispetto degli obblighi di riservatezza contenute nei contratti (assunzione del personale) e/o atti di nomina (dipendenti chiamati a ricoprire il ruolo di commissario/presidente/segretario di gara, RdP/DdE).

  Inoltre la Società adotta una misura specifica con particolare riferimento ai soggetti chiamati a governare la procedura di gara, venuti a conoscenza, in ragione della propria funzione, di informazioni sensibili per il mercato: - il Registro delle persone che hanno accesso alle informazioni privilegiate, recante i nomi delle persone che detengono e/o hanno accesso alle informazioni relative alla gara.

- ✓ Formazione: Su proposta del RPCT, l'AD approva annualmente il "*Piano integrato della formazione*" idoneo a garantire la corretta selezione e formazione del personale con riguardo alle tematiche relative all'anticorruzione, alla trasparenza, all'antiriciclaggio e alla privacy.

  Sono previste diverse tipologie di formazione, erogata da personale qualificato, da organizzarsi periodicamente in corsi d'aula o con altre soluzioni che garantiscano il riscontro dell'avvenuta formazione: formazione generale, diretta all'analisi della normativa di riferimento e rivolta a tutti i dipendenti e collaboratori; formazione specifica, maggiormente connessa al ruolo aziendale e rivolta a RPCT – OdV – DPO – GSOS -Membri CdA – Dirigenti - Referenti per l'anticorruzione e Referenti per la trasparenza - Focal points; formazione tecnica attinente a tematiche tecniche specifiche, connesse a determinati incarichi o ruoli aziendali (es. membro commissione di gara o RdP).

- ✓ Informatizzazione del processo: automatizzazione del processo/fase attraverso il sistema informatico.

- ✓ Whistleblowing: sistema di segnalazione di condotte illecite di cui il lavoratore sia venuto a conoscenza in ragione del proprio rapporto di lavoro all'interno della Pubblica Amministrazione. La Società utilizza una piattaforma informatica integrata che, in linea con le disposizione della Legge sopra illustrata, permette, tra l'altro, di gestire le comunicazioni/segnalazioni pervenute con garanzia di riservatezza per i soggetti segnalanti e la massima sicurezza informatica; tale piattaforma consente, al contempo, di interloquire con il soggetto segnalante - sia interno che esterno alla Società - e di rendicontare lo stato di avanzamento dell'istruttoria, se avviata, nel rispetto di quanto indicato dalle Linee guida ANAC in materia. Le comunicazioni/segnalazioni possono essere inviate al RPCT e/o all'OdV, a seconda della competenza, attraverso l'apposita piattaforma.

- ✓ Certificazioni: attestazione di rispondenza a specifici principi. La Società ha adottato un Sistema di Gestione per la Qualità nel rispetto dei principi della norma UNI EN ISO 9001. Include la certificazione ISO 9001:2015 del SGQ aziendale, ed in particolare i processi necessari per la realizzazione delle iniziative per l'acquisizione di beni e servizi - ovvero Convenzioni, MePa, SdaPa, Accordi quadro, Sistemi dinamici di acquisizione e acquisizioni su delega.

- ✓ Sistema disciplinare: Sistema Disciplinare, approvato dal CdA, idoneo a sanzionare il mancato rispetto delle misure previste dal Modello ex d.lgs. 231/01, dal Codice etico, dal PTPC. Il tipo e l'entità delle sanzioni sono variabili in relazione alla gravità dei comportamenti e tengono conto del principio di proporzionalità previsto dall'art. 2106 del codice civile.

- ✓ Sistema procedurale interno: Insieme delle procedure aziendali. La Società ha creato un repository sulla intranet aziendale c.d. "Processi e Procedure", finalizzata a consentire una visione d'insieme dei processi, collocandoli in uno schema di riferimento, con l'obiettivo di diffondere e agevolare la comprensione e la conoscenza del modello dei processi e, quindi, accrescerne performance ed efficienza.

- ✓ Accordi/Contratti: strumenti mediante i quali una determinata attività/fase di un processo viene posta in capo o demandata ad un soggetto terzo. Include i patti d'integrità.

- ✓ Accesso civico semplice e generalizzato: sistema adottato dalla Società per la gestione dell'acceso civico, sia semplice che generalizzato.
  - *Accesso civico semplice*: diritto riconosciuto a chiunque di richiedere documenti, informazioni o dati, oggetto di pubblicazione obbligatoria ai sensi del Decreto trasparenza, nei casi in cui sia stata omessa la loro pubblicazione (art. 5, comma 1, d.lgs. 33/13).
  - *Accesso civico generalizzato*: diritto riconosciuto a chiunque di richiedere documenti, informazioni o dati detenuti dalla Società, ulteriori rispetto a quelli oggetto di pubblicazione obbligatoria ai sensi del Decreto trasparenza (art. 5, comma 2, d.lgs. 33/13).

Include:

- un Regolamento recante «*Misure Organizzative Sul Diritto di Accesso Civico Semplice e Generalizzato*», che disciplina le modalità di esercizio del diritto di accesso e le relative limitazioni; tale Regolamento è pubblicato nell'apposita sezione in Società Trasparente
- un Registro delle istanze pervenute, al cui interno vengono riportati anche i relativi riscontri. Tale Registro, gestito dalla Divisione Compliance e Societario, è pubblicato semestralmente nell'apposita sezione prevista in Società Trasparente.

✓ Trasparenza: regole definite per garantire la trasparenza così come definita dal d. lgs 33/2013 e/o ulteriori norme specifiche. *minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza".*

Nel PTPC, nella sezione Trasparenza, sono riportate le strutture coinvolte ai fini della trasmissione, dell'aggiornamento e della pubblicazione dei dati, specificando la tempistica e la durata della pubblicazione.

✓ Disciplina revolving doors: strumenti adottati dalla Società al fine di disciplinare l'istituto del *revolving doors* di cui all'art. 53 comma 16-ter del d. lgs. 165/2001 che prevede espressamente il seguente divieto:

I dipendenti che, negli ultimi tre anni di servizio, hanno esercitato poteri autoritativi o negoziali per conto delle pubbliche amministrazioni di cui all'articolo 1, comma 2, non possono svolgere, nei tre anni successivi alla cessazione del rapporto di pubblico impiego, attività lavorativa o professionale presso i soggetti privati destinatari dell'attività della pubblica amministrazione svolta attraverso i medesimi poteri.

Include:

- accertamento della sussistenza o meno delle cause ostative di cui all'art. 53, c. 16-ter del d.lgs. 165/2001, per la stipula di un contratto di lavoro (autonomo o subordinato) o per il conferimento di un incarico mediante apposite dichiarazioni ad evento (attività precedente all'assunzione/conferimento incarico);
- dichiarazioni rese al momento della cessazione del rapporto di lavoro (attività successiva - rispetto del divieto di *pantouflage* nei tre anni successivi alla cessazione del rapporto di lavoro con la Società);
- clausole specifiche nei bandi di gara.

CAPITOLO 5

L'ORGANISMO DI VIGILANZA

5.1 CARATTERISTICHE GENERALI DELL'ORGANISMO DI VIGILANZA DELLA SOCIETÀ

L'articolo 6, lettera b), del Decreto riconosce efficacia esimente dalla responsabilità amministrativa a favore dell'ente che affida ad un *organismo interno, dotato di autonomi poteri di iniziativa e di controllo*, il compito di vigilare:

- sull'efficacia e adeguatezza del Modello in relazione alla struttura aziendale ed all'effettiva capacità di prevenire la commissione dei reati;
- sull'osservanza delle prescrizioni del Modello da parte dei suoi Destinatari;
- sull'opportunità di aggiornamento del Modello, laddove si riscontrino esigenze di adeguamento in relazione a mutate condizioni aziendali e/o normative.

L'istituzione di tale Organismo è condizione imprescindibile per l'esonero di responsabilità dell'ente; a tal fine l'OdV deve essere in possesso di determinati e specifici requisiti quali, autonomia ed indipendenza, professionalità, onorabilità e continuità di azione.

Per garantire autonomia e indipendenza, secondo una concreta interpretazione delle norme, l'Organismo di Vigilanza di Consip è posto *all'esterno dei processi operativi* della Società, in posizione di staff al Consiglio di Amministrazione, svincolato da ogni rapporto gerarchico con i singoli responsabili delle Divisioni ed Aree/Funzioni aziendali di Consip.

5.1.a) Caratteristiche

In considerazione di quanto sopra, il Consiglio di Amministrazione della Società ha affidato il relativo incarico ad un Organismo collegiale misto, composto da soggetti esterni ed interni all'azienda, appositamente istituito, i cui membri siano in possesso delle seguenti caratteristiche:

a. ***autonomia***, intesa come:
   - ✓ soggettività funzionale autonoma, in quanto l'OdV non svolge attività proprie di altre funzioni aziendali;
   - ✓ possesso di autonomi poteri e capacità di iniziativa e controllo;
   - ✓ assenza di compiti operativi;
   - ✓ collocazione in posizione di staff al Consiglio di Amministrazione;
   - ✓ possibilità di relazionarsi direttamente con tutti i soggetti che svolgono attività per conto di Consip;

b. ***professionalità***, intesa come bagaglio di conoscenze, strumenti e tecniche che l'Organismo di Vigilanza (così come i suoi membri) deve possedere, in modo da poter efficacemente eseguire in concreto la funzione di vigilanza negli ambiti di competenza funzionalmente collegati alle attività che è chiamato a svolgere (es. tematiche di economia, organizzazione aziendale, responsabilità amministrativa di impresa, nonché tematiche di natura legale idonee a garantire l'efficacia dei poteri di controllo);

c. *onorabilità,* considerata come assenza di cause di ineleggibilità o decadenza previste dall'art. 2382 c.c. e delle ulteriori definite dalla giurisprudenza o dal presente Modello;

d. *continuità di azione*, da realizzarsi attraverso la presenza nell'Organismo di Vigilanza di almeno una persona interna all'organizzazione della Società.

5.1.b) Requisiti di professionalità

L'OdV, nella sua composizione, deve possedere i seguenti requisiti professionali:

- competenze ed esperienze specifiche in ambito di d.lgs 231/2001 e/o di diritto penale dell'economia e dell'impresa;
- competenze in materia di controlli interni e procedure aziendali;

idonee a garantire l'efficacia dei poteri di controllo e del potere propositivo demandato all'organismo di cui fanno parte.

5.1.c) Requisiti di onorabilità

I membri dell'OdV devono possedere i seguenti requisiti di onorabilità e non devono incorrere nelle ipotesi di incompatibilità nel seguito indicate:

a) pieno godimento dei diritti civili e politici;

b) capacità di contrarre con la Pubblica Amministrazione;

c) assenza di cause di ineleggibilità o decadenza previste dall'art. 2382 c.c.;

d) assenza di provvedimento di condanna anche non definitiva o con pena condizionalmente sospesa/sentenza di "patteggiamento", fatti salvi gli effetti della riabilitazione, per taluno dei delitti previsti da (in analogia a quanto definito anche per i membri del CdA):
   - R.D. 16/03/1942, n. 267 (Disciplina del fallimento, del concordato preventivo, dell'amministrazione controllata e della liquidazione coatta amministrativa);
   - titolo XI del libro V del codice civile (reati societari);
   - norme che individuano i delitti contro la Pubblica Amministrazione, contro la fede pubblica, contro il patrimonio, contro l'ordine pubblico, contro l'economia pubblica e in materia tributaria;
   - norme che disciplinano l'attività bancaria, finanziaria, mobiliare, assicurativa e dalle norme in materia di mercati e valori mobiliari, di strumenti di pagamento;
   - norme che disciplinano l'associazione per delinquere in materia di immigrazione/associazione di stampo mafioso/disciplina degli stupefacenti e sostanze psicotrope (art. 51, comma 3-bis, c.p.p. – art. 73 del Decreto del Presidente della Repubblica 9 ottobre 1990, n. 309);

e) assenza di provvedimento di condanna, anche non definitiva o con pena condizionalmente sospesa/sentenza di "patteggiamento" per la commissione di reati presupposto ex d.lgs. 231/2001 o la commissione dolosa di un danno erariale;

f) assenza di misure cautelari personali, coercitive o interdittive, per i reati previsti dal d.lgs. 231/2001;

g) assenza di condanna anche non definitiva, ovvero di sentenza di "patteggiamento", a una pena che importa l'interdizione, anche temporanea, o la sospensione dai pubblici uffici, ovvero l'interdizione temporanea dagli uffici direttivi delle persone giuridiche e delle imprese;

h) assenza di misure di prevenzione ai sensi del d.lgs. n. 159/2011 (normativa antimafia);

i) assenza di condanne penali e/o di provvedimenti che riguardano l'applicazione di misure di prevenzione e/o di procedimenti penali in corso;

j) non essere, o non essere stato, in uno dei tre esercizi precedenti, un componente del Consiglio di Amministrazione di Consip S.p.A.;

k) non avere[34], o non aver avuto, direttamente o indirettamente, in uno dei tre esercizi precedenti, rapporti commerciali, finanziari o professionali rilevanti con la Società;

l) non avere, o non aver avuto, direttamente o indirettamente, in uno dei tre esercizi precedenti, rapporti commerciali, finanziari o professionali rilevanti con i componenti del Consiglio di Amministrazione, con i responsabili di Divisione della Società e con i membri del Collegio sindacale;

m) assenza di rapporti di parentela, coniugio/convivenza o affinità entro il II grado con i componenti del Consiglio di Amministrazione, con i responsabili di Divisione della Società e con i membri del Collegio sindacale;

n) assenza di conflitti di interesse permanenti con la Società che danneggino l'indipendenza e l'autonomia del componente dell'OdV;

o) assenza di ogni ulteriore causa di incompatibilità espressamente prevista da disposizioni di legge o regolamentari;

p) non aver subito, negli ultimi 5 anni, provvedimenti disciplinari irrogati dall'Ordine professionale di appartenenza.

5.2 NOMINA DELL'ODV

Il Consiglio di Amministrazione di Consip provvede alla nomina dell'Organismo di Vigilanza adottando apposita delibera.

Ai fini della composizione dell'Organismo di Vigilanza, sebbene non obbligatorio per legge, il Consiglio di Amministrazione tiene in considerazione anche il rispetto dell'equilibrio di genere, in analogia con quanto prescritto dalla normativa vigente per la nomina del Consiglio stesso e del Collegio Sindacale della Società, la quale prevede che il genere meno rappresentato ottenga almeno 1/3 di ciascun organo sociale (art. 2 D.P.R. 251/2012 Regolamento attuativo della L. 120/2011.

Il Consiglio di Amministrazione all'atto della nomina:

✓ ne determina la durata in carica, di regola non inferiore ai tre anni (salvo eccezioni motivate);

[34] Fatta eccezione per il rapporto di lavoro subordinato preesistente.

- ✓ definisce gli emolumenti dei componenti;
- ✓ designa il Presidente dell'OdV (il "**Presidente**"), scegliendolo tra membri esterni, cui è affidato il compito di promuovere e coordinare l'attività dell'OdV.

I membri dell'OdV sono rinnovabili, fino ad un massimo di n. 2 mandati.

L'Organismo cessa per scadenza del termine alla data dell'assemblea convocata per l'approvazione del bilancio relativo all'ultimo esercizio della sua carica, pur continuando a svolgere ad interim le proprie funzioni (in regime di cd. *prorogatio*) fino a nuova nomina dei componenti dell'Organismo stesso, così da garantire la continuità dell'azione.

I membri dell'OdV restano in carica per tutta la durata del mandato ad essi conferito, indipendentemente dalle variazioni riguardanti la composizione del Consiglio di Amministrazione che li ha nominati.

È rimessa al C.d.A. della Società la valutazione periodica circa l'adeguatezza dell'Organismo di Vigilanza in termini di struttura organizzativa e di poteri conferiti, apportando, mediante delibera consiliare, le modifiche e/o integrazioni ritenute necessarie.

5.3 DECADENZA E SOSTITUZIONE DEI COMPONENTI DELL'ODV

Comportano la decadenza automatica dalla carica di componente dell'OdV la ricorrenza di una delle cause di ineleggibilità, nonché il venir meno dei requisiti di onorabilità e professionalità di cui al precedente art. 5.1.

I componenti dell'OdV sono tenuti a comunicare immediatamente al Consiglio di Amministrazione ed allo stesso OdV l'insorgere di eventuali condizioni ostative al permanere dei requisiti necessari alla carica.

Il Consiglio di Amministrazione, al di fuori dei casi di incompatibilità e/o ineleggibilità, può revocare la nomina alla carica di membro o di Presidente dell'OdV soltanto per giusta causa, quale:

- violazione, da parte dell'OdV o di taluno dei suoi membri, di prescrizioni e/o regole comportamentali stabilite nel Modello;
- attribuzione di funzioni e responsabilità operative all'interno dell'organizzazione aziendale, comunque incompatibili con i requisiti di autonomia e continuità di azione propri dell'OdV.

Al verificarsi di un presupposto o condizione che comporti la sostituzione di un componente dell'OdV, è data comunicazione tempestiva al Consiglio di Amministrazione della Società, che provvede, senza indugio, alla sostituzione. Il membro così nominato resterà in carica sino alla data di scadenza naturale dell'OdV.

5.4 FUNZIONI, POTERI E COMPITI DELL'ODV

L'OdV, in adempimento della delega ricevuta, deve:

- ✓ vigilare sull'effettiva e concreta applicazione del Modello, verificando la congruità dei

comportamenti all'interno della Società rispetto allo stesso;

- ✓ monitorare sulla effettiva attuazione del Modello per prevenire la commissione dei reati di cui al Decreto;
- ✓ proporre e promuovere tutte le iniziative necessarie alla conoscenza del presente Modello;
- ✓ valutare la concreta adeguatezza nel tempo del Modello a svolgere la sua funzione di strumento di prevenzione dei reati;
- ✓ proporre alla Società le necessarie modifiche/integrazioni al Modello;
- ✓ verificare l'attuazione e l'effettiva funzionalità delle modifiche apportate al Modello;
- ✓ verificare che i protocolli previsti dal Modello siano adeguati e rispondenti alle necessità di osservanza delle prescrizioni del Decreto promuovendone, in caso contrario, la necessità di aggiornamento;
- ✓ eseguire periodicamente verifiche ispettive, anche a sorpresa, non esclusivamente documentali, volte all'accertamento di quanto previsto nel Modello;
- ✓ relazionare agli organi competenti con cadenza almeno semestrale sulle attività di vigilanza svolte e sullo stato di attuazione del Modello (cfr capitolo 5.4.a);
- ✓ disporre, a sua discrezione, l'audizione di risorse che possano fornire le informazioni o indicazioni utili;
- ✓ partecipare al processo di gestione integrata del rischio per quanto di competenza, collaborando con il RPCT (cfr capitolo 4);
- ✓ coordinarsi con il RPCT in caso di eventi rilevanti ai sensi della L. 190/2012 e del d.lgs. 231/01, oltre che nella gestione dei flussi (cfr capitolo 5.4);
- ✓ ricevere le segnalazioni - ed effettuare la relativa istruttoria unitamente al RPCT - di cui al sistema di whistleblowing (cfr capitolo 6);
- ✓ dirimere eventuali incertezze interpretative del Codice Etico;
- ✓ coordinarsi con il RPCT ai fini della diffusione del Codice etico e del monitoraggio sull'attuazione dello stesso, ivi incluse le comunicazioni relative al conflitto di interessi, effettuando i necessari approfondimenti;
- ✓ esprimere valutazione di adeguatezza del Piano Integrato della Formazione, coordinandosi con gli altri organi di controllo e la DCS (cfr capitolo 8.1);
- ✓ coordinarsi con il RPCT, la DCS e la DIA ai fini della definizione del Piano Integrato dei Controlli (cfr capitolo 7.1).

Ai fini dello svolgimento dei propri compiti, l'OdV può emanare disposizioni tese a:

a) regolamentare la propria attività, anche attraverso l'adozione di un **Regolamento interno di funzionamento**, volto a indicare la disciplina delle attività operative dell'OdV;

b) specificare le modalità attuative dei flussi informativi da e verso l'OdV, come stabiliti dal Modello.

Di tale circostanza l'OdV informa prontamente il Consiglio di Amministrazione di Consip.

L'Organismo di Vigilanza si riunisce periodicamente, almeno otto volte all'anno, per verificare lo stato di avanzamento delle attività di verifica in corso, predisporre la documentazione dovuta, attivare le nuove iniziative, valutare i fatti riscontrati e decidere in merito alle possibili azioni da compiere.

Tenuto conto delle peculiari funzioni attribuite all'OdV e dei contenuti professionali specifici necessari, nello svolgimento dei propri compiti di vigilanza e controllo, l'OdV si avvale del supporto della Divisione Internal Audit e alla Divisione Compliance e Societario, per quanto di rispettiva competenza.

All'Organismo di Vigilanza viene inoltre assicurata, in conformità con le procedure aziendali, una dotazione finanziaria (*budget*) adeguata per permettere a quest'ultimo di espletare al meglio la propria funzione. A tal proposito, nel rispetto delle procedure aziendali, potrà avvalersi per il perseguimento dei fini istituzionali a cui è preposto del supporto di soggetti esterni il cui contributo specialistico si renda, di volta in volta, necessario.

5.5 REPORTING E FLUSSI

5.5.a) Reporting dell'Organismo di Vigilanza ed incontri periodici

L'OdV riporta direttamente al Consiglio di Amministrazione della Società e riferisce in merito all'attuazione del Modello e ad ogni eventuale criticità nell'ottica della prevenzione del rischio reato e del rispetto del Codice Etico aziendale. In particolare, l'OdV provvede:

a) a redigere un rapporto operativo semestrale al Consiglio di Amministrazione, nel quale sono specificati gli interventi effettuati, le criticità riscontrate e lo stato di implementazione delle misure preventive previste nel Modello, nonché degli interventi correttivi e migliorativi suggeriti o pianificati;

b) nell'ambito della relazione semestrale di cui sopra, alla consuntivazione delle attività svolte nel semestre di riferimento ed alla pianificazione delle attività per il semestre successivo.

La relazione viene inviata, per quanto di rispettiva competenza, anche al Collegio sindacale, al RPCT, al DP, al DPO, al GSOS, all'OIV e al responsabile della Divisione Internal Audit.

In ogni caso, l'OdV deve riferire tempestivamente al Consiglio di Amministrazione in merito a qualsiasi violazione del Modello, di cui sia venuto a conoscenza per effetto di una segnalazione, ritenuta fondata, o che abbia accertato durante lo svolgimento delle proprie attività; l'OdV ha dunque facoltà di richiedere, attraverso le funzioni o i soggetti competenti, l'audizione al Consiglio di Amministrazione per motivi urgenti, purché inerenti alle proprie mansioni istituzionali.

Il Consiglio di Amministrazione ha la facoltà di convocare in qualsiasi momento l'OdV per essere informato e aggiornato su fatti o tematiche inerenti all'applicazione del Modello ed, in genere,

del d.lgs. 231/2001.

5.5.b) Rapporti tra OdV e altri organi di controllo

L'OdV incontra almeno una volta l'anno (i) il Collegio Sindacale e (ii) il Responsabile del Sistema di Sicurezza dei Lavoratori (RSSL), per verificare il corretto espletamento delle attività in materia di sicurezza dei lavoratori.

In generale l'OdV opera in stretta correlazione con il RPCT, ognuno per quanto di rispettiva competenza, al fine di garantire la necessaria cooperazione ed integrazione: il RPCT definisce, in accordo con l'OdV, appositi flussi informativi tra le due funzioni; in particolare lo stesso RPCT e l'OdV si scambiano informazioni relative a fatti o circostanze apprese nell'esercizio delle loro specifiche funzioni in materia di violazioni del Modello e del PTPC, se di reciproco interesse.

L'OdV può, inoltre, utilmente segnalare al RPCT situazioni non direttamente rilevanti ai sensi e per gli effetti della L. 190/12 o del d.lgs. 231/2001, ma di potenziale attinenza al sistema dei controlli introdotti dal Modello.

Ai fini di cui sopra, il RPCT può inoltre partecipare alle riunioni periodiche dell'OdV.

In ogni caso l'OdV incontra o si relaziona con ogni Direzione o Area/Funzione, o organismo aziendale che ne faccia richiesta allo scopo di migliorare l'attuazione del Modello e/o promuovere la diffusione della cultura di prevenzione del rischio reato.

Inoltre, al fine di garantire il necessario coordinamento con gli altri organi di controllo della Società, l'OdV riceve i Report e le Relazioni periodiche del RPCT, dell'OIV, della Divisione Internal Audit, del DP, del DPO e del GSOS; nello specifico:

- risultati del *risk assessment integrato*
- report sui controlli/*audit* effettuati dalle strutture aziendali della Società nell'ambito della loro attività di controllo (Report Area IA, verifiche Dirigente Preposto, verifiche Qualità, ecc)
- relazione semestrale del DP
- relazione semestrale del RPCT
- relazione semestrale della Divisione Internal Audit
- Relazione periodica del DPO
- Relazione periodica del GSOS
- relazione annuale dell'OIV.

5.5.c) Reporting vs l'OdV

Nell'ottica di garantire l'integrazione tra gli organismi di controllo, ciascun Referente, con riguardo alla Divisione di competenza, aggiorna con cadenza periodica il RPCT, il DPO, il GSOS e l'OdV sullo stato di attuazione delle misure preventive o sulle eventuali criticità/violazioni riscontrate, compilando uno specifico schema di report a questi sottoposto.

5.5.d) Flussi vs il RPCT e OdV

Il RPCT ha definito, unitamente all'OdV e ad integrazione del Report di cui sopra, l'elenco dei flussi informativi verso i due Organismi, individuando per ognuno (i) tipologia, (ii) oggetto, (iii) responsabile invio, (iv) frequenza e (v) destinatario.

L'elenco dei flussi viene aggiornato annualmente da RPCT/OdV, laddove necessario.

I Referenti garantiscono tali flussi verso il RPCT/OdV; il mancato rispetto di tale obbligo viene sanzionato in base al Sistema disciplinare, allegato al Modello.

CAPITOLO 6

WHISTLEBLOWING

6.1 CONTESTO NORMATIVO

Con l'art. 1, comma 51, la Legge 190/2012 disciplina il c.d. *whistleblowing*, cioè la segnalazione di condotte illecite di cui il lavoratore (*whistleblower* - letteralmente "soffiatore nel fischietto") sia venuto a conoscenza in ragione del proprio rapporto di lavoro all'interno della Pubblica Amministrazione. Come dimostra l´esperienza maturata in altri paesi (es. Gran Bretagna e Stati Uniti), il *whistleblowing* rappresenta uno strumento potenzialmente determinante per contrastare i fenomeni corruttivi attraverso l´incremento del tasso di denuncia. La stessa ANAC ha più volte ribadito l´importanza di questo canale informativo, quale imprescindibile veicolo per scongiurare o arrestare tempestivamente la commissione di fatti illeciti, sottolineando al contempo l'importanza degli strumenti di tutela dell´identità dell´informatore forniti dalla norma, che incoraggiano in tal modo eventuali *whistleblowers* che desiderino preservare la riservatezza. La *ratio* della norma è evidentemente quella di evitare che il dipendente ometta di effettuare segnalazioni di illecito per il timore di subire conseguenze pregiudizievoli.

L'art. 54-bis del d.lgs. 165/2001, richiamato dalla Legge 190/2012, nel definire tutta una serie di presidi a garanzia del dipendente pubblico che segnala illeciti, stabilisce, inoltre, che anche ANAC è chiamata a gestire, oltre alle segnalazioni provenienti dai propri dipendenti per fatti illeciti avvenuti all'interno della propria struttura, anche le segnalazioni che i dipendenti di altre amministrazioni possono indirizzarle. Dal 22 ottobre 2014 ANAC ha dunque aperto "*un canale privilegiato (whistleblowing@anticorruzione.it) a favore di chi, nelle situazioni di cui si è detto, scelga di rivolgersi all'Autorità e non alle vie interne stabilite dalla Pubblica Amministrazione di appartenenza. É stato quindi istituito un protocollo riservato dell'Autorità, in grado di garantire la necessaria tutela del pubblico dipendente: sono assicurati la riservatezza sull'identità del segnalante e lo svolgimento di un'attività di vigilanza, al fine di contribuire all'accertamento delle circostanze di fatto e all'individuazione degli autori della condotta illecita*."

Con Determinazione n. 6 del 28 aprile 2015, ANAC aveva emanato le "*Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)*"; in tale contesto ANAC, nel rilevare la mancanza di una specifica previsione normativa relativa alla tutela dei dipendenti che segnalano condotte illecite negli enti di diritto privato in controllo pubblico e negli enti pubblici economici, sottolineava l'opportunità che le amministrazioni controllanti e vigilanti promuovessero da parte dei suddetti enti, eventualmente nell'ambito del Piano di prevenzione della corruzione, l'adozione di misure di tutela analoghe a quelle previste nelle citate Linee guida. Le stesse Linee guida ANAC per le società (cap. 2.1.) rilevavano che "*In mancanza di una specifica previsione normativa relativa alla tutela dei dipendenti che segnalano illeciti nelle società, come già rappresentato nelle Linee guida in materia emanate dall'Autorità con determinazione n. 6 del 28 aprile 2015, le amministrazioni controllanti promuovono l'adozione da parte delle società di misure idonee ad incoraggiare il dipendente a denunciare gli illeciti di cui viene a conoscenza nell'ambito del rapporto di lavoro, avendo cura di garantire la riservatezza dell'identità del*

segnalante dalla ricezione e in ogni contatto successivo alla segnalazione. A questo fine è utile assicurare la trasparenza del procedimento di segnalazione, definendo e rendendo noto l'iter, con l'indicazione di termini certi per l'avvio e la conclusione dell'istruttoria e con l'individuazione dei soggetti che gestiscono le segnalazioni.".

Successivamente è stata emanata la Legge 30 novembre 2017, n. 179 recante "*Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"*, che modifica alcuni aspetti della normativa in ambito pubblico (art. 54-bis del d.lgs. 165/2001) ed estende la disciplina del *whistleblowing* al settore privato (art. 6 del d.lgs. 231/2001). Con tali modifiche il Legislatore ha innanzitutto chiarito, per quanto rileva ai fini della disciplina applicabile alla Società, che per dipendente pubblico si debba intendere anche il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile, sottolineando altresì che tale disciplina si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica. La Legge ha, inoltre, introdotto una serie di misure organizzative poste a tutela del segnalante e relative sanzioni, prevedendo, altresì, l'adozione di sistemi informativi - che Consip ha opportunamente adottato, come nel seguito meglio precisato - volti a tutelare l'identità del segnalante ed il contenuto della segnalazione. Nello specifico, le nuove norme prevedono che nei confronti del dipendente che segnali illeciti al RPCT/OdV, all'ANAC o ai magistrati ordinari e contabili, non possano essere disposte misure discriminatorie quali, ad esempio, demansionamento, licenziamento, trasferimento, sanzioni ecc.. In caso di licenziamento viene previsto il reintegro nel posto di lavoro e, comunque, la nullità di ogni atto discriminatorio o ritorsivo. La legge disciplina inoltre l'inversione dell'onere della prova, nel senso che spetta all'ente dimostrare l'estraneità della misura adottata rispetto alla segnalazione. Dal punto di vista sanzionatorio, viene stabilito che l'ANAC possa irrogare sanzioni pecuniarie in caso di applicazione di misure discriminatorie, ovvero qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni, o ancora laddove le stesse non risultino conformi alle Linee Guida dettate dall'ANAC. Infine, è prevista una sanzione specifica nei confronti del RPCT qualora venga accertato il mancato svolgimento delle attività di verifica e di analisi delle segnalazioni ricevute.

Attualmente si è in attesa che ANAC pubblichi le *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs 165/2001 (c.d. whistleblowing)* poste in consultazione in data 24 luglio 2019.

Per quanto attiene all'estensione della disciplina al settore privato, l'art. 6 del d.lgs. 231/2001, così come modificato, stabilisce che i Modelli ex d.lgs. 231/01 debbano prevedere:

a) uno o più canali che consentano di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti ai sensi del citato 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 devono garantire 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) la previsione di 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.

Infine, con l'art. 3 della L. 179/2017, il Legislatore ha modificato la disciplina del segreto d'ufficio, aziendale, professionale, scientifico e industriale in caso di *whistleblowing*, individuando, come giusta causa di rivelazione del segreto d'ufficio (art. 326 c.p.), professionale (art. 622 c.p.), scientifico e industriale (art. 623 c.p.), nonché di violazione dell'obbligo di fedeltà nei confronti dell'imprenditore (art. 2105 c.c.), il perseguimento dell'interesse all'integrità delle amministrazioni alla prevenzione e alla repressione delle malversazioni. Tale disposizione non si applica nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata. La norma precisa, inoltre, che quando le notizie e i documenti che sono comunicati nell'ambito del *whistleblowing,* sono oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

6.2 IL SISTEMA DI WHISTLEBLOWING

6.2.a) Sistema adottato

Consip, nell'ambito del Modello ex d.lgs. 231/01, aveva da tempo previsto alcuni canali per consentire la comunicazione da e verso l'OdV, sia relativamente ai dipendenti che ai soggetti esterni alla Società:

- ✓ una casella istituzionale di posta elettronica (odv@consip.it), a cui far confluire eventuali segnalazioni; tale indirizzo era pubblicato sul sito internet della Società, nella sotto-sezione dedicata all'Organismo di Vigilanza
- ✓ sulla intranet aziendale, nell'Area Società, una sezione dedicata all'Organismo di Vigilanza dove sono presenti, oltre alla normativa 231 e al Modello, anche tutti i riferimenti utili per contattare l'Organismo stesso.

Dato il tenore della norma ed il ruolo che viene riconosciuto al *whistleblowing* quale importante strumento di prevenzione della corruzione, Consip ha successivamente proseguito nel percorso già avviato:

- ✓ implementando un sistema di segnalazione ad uso dei dipendenti, che consentiva la gestione delle segnalazioni stesse sia da parte dell'OdV che del RPCT, ciascuno per quanto di rispettiva competenza, garantendo al tempo stesso la figura del *whistleblower*;
- ✓ consentendo anche ai soggetti esterni di effettuare comunicazioni/segnalazioni attraverso il medesimo sistema, andando così a sostituire le due caselle istituzionali di posta elettronica

dell'OdV e del RPCT, ai fini di una maggiore efficienza nella gestione delle comunicazioni/segnalazioni in generale da parte dei citati organi.

Anche tenendo conto delle indicazioni in materia fornite dall'ANAC, il RPCT, d'intesa con l'OdV, nel corso del 2016 aveva avviato un progetto per l'implementazione di un sistema evoluto di *whistleblowing* al fine di migliorare l'efficacia dello strumento e permettere una gestione più efficiente delle comunicazioni/segnalazioni ricevute e delle relative istruttorie, anche a maggiore tutela, a seconda della tipologia di soggetto segnalante, della riservatezza ovvero dell'anonimato del segnalante. Nel corso del 2017 è stata dunque acquisita una piattaforma informatica integrata *web-based,* basata sul *software Segnalazioni.net,* che*,* in linea con le disposizione della Legge sopra illustrata*,* permette, tra l'altro, di gestire le comunicazioni/segnalazioni pervenute con garanzia di riservatezza per i soggetti segnalanti e la massima sicurezza informatica; tale piattaforma consente, al contempo, di interloquire con il soggetto segnalante - sia interno che esterno alla Società - e di rendicontare lo stato di avanzamento dell'istruttoria, se avviata, nel rispetto di quanto indicato dalle Linee guida ANAC in materia.

Per l'anno 2020 sono previsti alcuni aggiornamenti della piattaforma informatica per lo più di carattere tecnico-operativo, utili a migliorare ulteriormente l'efficacia dello strumento ee a permettere una gestione ancor più efficiente delle segnalazioni.

6.2.b) Accesso al Sistema

Le comunicazioni/segnalazioni possono essere inviate al RPCT e/o all'OdV, a seconda della competenza, attraverso l'apposita piattaforma. L'accesso al nuovo Sistema di whistlebowing è consentito sia agli utenti registrati che agli utenti non registrati (anonimi), mediante il seguente indirizzo:

https://consip.segnalazioni.net

La Società rende accessibile il Sistema di whistleblowing:

- tramite il sito internet Consip, nell'apposita pagina denominata *"Whistleblowing"*;
- tramite il sito internet Consip, all'interno delle sotto-sezioni dedicate all'OdV e al RPCT nella sezione "Società Trasparente".

Del Sistema di whistleblowing viene inoltre data ampia e dettagliata comunicazione a tutto il personale ed ai collaboratori della Società, cui vengono fornite le indicazioni e le istruzioni necessarie per potervi accedere.

Resta ovviamente inteso che le segnalazioni pervenute verranno valutate, con le modalità di cui al successivo cap. 7 *"Monitoraggio, controlli e reportistica"*, anche se provenienti attraverso canali differenti (es. a mezzo posta).

6.2.c) Gestione delle segnalazioni

Per la gestione del Sistema di whistleblowing e delle singole comunicazioni/segnalazioni, l'OdV e il RPCT si avvalgono del supporto della Divisione Compliance e Societario (DCS) e della Divisione

Internal Audit (DIA), per quanto di rispettiva competenza. Per il dettaglio dell'iter istruttorio si rimanda al relativo cap. 7*"Monitoraggio, controlli e reportistica"*.

I dati e i documenti oggetto della comunicazione/segnalazione vengono trattati nel rispetto della normativa in materia di protezione dei dati personali ed in base alle disposizioni contenute nel Sistema privacy della Società.

L'OdV e il RPCT garantiscono la gestione dell'istruttoria nel rispetto delle norme di riservatezza e dei principi di garanzia dell'anonimato; in particolare:

- laddove necessario, separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi in cui ciò sia strettamente necessario;
- nella piattaforma informatica, viene sempre garantita la riservatezza del segnalatore, mediante separazione dei dati identificativi del segnalante dal contenuto della segnalazione in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi in cui ciò sia strettamente necessario e sia previsto dalla legge;
- non permettere di risalire all'identità del segnalante se non nei casi espressamente stabiliti dalla normativa vigente (cfr cap. 6.5 *"Tutela del whistleblower"*);
- mantenere riservato, per quanto possibile, anche in riferimento alle esigenze istruttorie, il contenuto della segnalazione durante l'intera fase di gestione della stessa.

L'OdV e/o il RPCT comunicano lo stato dell'istruttoria (archiviazione - istruttoria in corso – istruttoria conclusa) al segnalante, laddove da questi richiesto. In caso di segnalazione effettuata tramite piattaforma, il segnalante può visionare lo stato in ogni momento (non letta - letta - in lavorazione - archiviata).

6.2.d) Contenuti delle segnalazioni

Come indicato nelle Linee guida ANAC in materia, le condotte illecite oggetto di segnalazione "*comprendono non solo l'intera gamma dei delitti contro la pubblica amministrazione di cui al Titolo II, Capo I, del codice penale (ossia le ipotesi di corruzione per l'esercizio della funzione, corruzione per atto contrario ai doveri d'ufficio e corruzione in atti giudiziari, disciplinate rispettivamente agli artt. 318, 319 e 319-ter del predetto codice), ma anche le situazioni in cui, nel corso dell'attività, si riscontri l'abuso da parte di un soggetto del potere a lui affidato al fine di ottenere vantaggi privati, nonché i fatti in cui – a prescindere dalla rilevanza penale – venga in evidenza un mal funzionamento a causa dell'uso a fini privati delle funzioni attribuite [……] Si pensi, a titolo meramente esemplificativo, ai casi di sprechi, nepotismo, demansionamenti, ripetuto mancato rispetto dei tempi procedimentali, assunzioni non trasparenti, irregolarità contabili, false dichiarazioni, violazione delle norme ambientali e di sicurezza sul lavoro. Le condotte illecite segnalate, comunque, devono riguardare situazioni di cui il soggetto sia venuto direttamente a conoscenza «in ragione del rapporto di lavoro» e, quindi, ricomprendono certamente quanto si è*

appreso in virtù dell'ufficio rivestito ma anche quelle notizie che siano state acquisite in occasione e/o a causa dello svolgimento delle mansioni lavorative, seppure in modo casuale" [35].

A supporto di quanto sopra, la L. 179/2017 conferma che le segnalazioni inviate nell'interesse dell'integrità dell'ente devono essere riferite a condotte illecite di cui il segnalante sia venuto a conoscenza in ragione del rapporto di lavoro. Si rammenta, inoltre, come l'art. 3 della citata legge disponga che la segnalazione o denuncia effettuata nelle forme e nei limiti di cui all'art. 54-bis e all'art. 6 del d.lgs. 231/01 per il perseguimento dell'interesse all'integrità della Società, nonché per la prevenzione e la repressione delle malversazioni, costituisce giusta causa di rivelazione di notizie coperte dall'obbligo di segreto di cui agli artt. 326, 622 e 623 del codice penale e all'art. 2105 del codice civile (obbligo del segreto d'ufficio, aziendale, professionale, scientifico e industriale). Come già sopra indicato, si ribadisce inoltre che quando le notizie e i documenti, che sono comunicati nell'ambito del *whistleblowing,* sono oggetto di segreto aziendale, professionale o d'ufficio, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

Qualora venga utilizzato il Sistema di whistleblowing, il segnalante può classificare la comunicazione/segnalazione in base alla natura del presunto illecito.

Le segnalazioni devono essere il più possibile circostanziate e offrire il maggior numero di elementi, al fine di consentire al RPCT e/o all'OdV di effettuare le dovute verifiche. Per quanto riguarda le segnalazioni anonime, si rinvia al successivo par. 6.4 *"Segnalazioni anonime"*.

Le segnalazioni devono essere il più possibile circostanziate e offrire il maggior numero di elementi[36], al fine di consentire al RPCT e/o all'OdV di effettuare le dovute verifiche.

L'Anac nelle Linee Guida del 24 luglio 2019, attualmente in pubblicazione, ha inoltre chiarito che non è necessario che il dipendente sia certo dell'effettivo accadimento dei fatti denunciati e/o dell'identità dell'autore degli stessi; è infatti sufficiente che il dipendente, in base alle proprie

[35]Le Linee Guida Anac del 24 luglio 2019, in pubblicazione, nella Parte Prima cap. 2.1 "*Condotte illecite"* forniscono un'elencazione esemplificativa di condotte illecite oggetto delle segnalazioni meritevoli di tutela*: comportamento non conforme ai doveri di ufficio (es. mancato rispetto delle disposizioni di servizio); accesso indebito ai sistemi informativi (anche mediante l'utilizzo di credenziali altrui); utilizzo improprio di istituti a tutela del dipendente (es. malattia, garanzie e tutele ex legge 5 febbraio 1992 n. 104, congedi, permessi sindacali); irregolarità e utilizzo distorto del potere discrezionale nell'ambito di procedure di affidamento di contratti pubblici e irregolarità nello svolgimento di procedimenti amministrativi che comportano uno scorretto utilizzo dell'esercizio del potere discrezionale a fini meramente privati, in contrasto con il fine pubblico; rapporti/frequentazioni inopportune tra dipendenti ed "esterni" per il raggiungimento di fini privati, mediante l'abuso della posizione pubblica attribuita (es. contribuenti, utenti, consulenti, etc.); erronea classificazione di spese in bilancio e/o mancato accantonamento di fondi; autorizzazione e liquidazione indebita di spese relative al personale.*

[36]Le Linee Guida Anac del 24 luglio 2019, in pubblicazione, nella Parte Prima cap. 2.2 prevedono espressamente che " *è necessario che la segnalazione sia il più possibile circostanziata al fine di consentire la delibazione dei fatti da parte del RPCT o di ANAC. In particolare devono risultare chiare le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione; la descrizione del fatto; le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati. E' utile anche allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di segnalazione, nonché l'indicazione di soggetti che possano contribuire a formare un quadro il più completo possibile di quanto segnalato"*.

conoscenze, ritenga ragionevolmente che una irregolarità o un fatto illecito si sia verificato. Può altresì formare oggetto di segnalazione un'attività illecita intrapresa, ma non ancora perfezionatasi, in presenza di elementi precisi e concordanti prodromici all'attività stessa.

6.3 SEGNALAZIONI PROVENIENTI DA UTENTI REGISTRATI

Per effettuare una segnalazione all'OdV e/o al RPCT, il personale interno e i collaboratori della Società possono accedere al Sistema di whistleblowing, utilizzando le proprie credenziali (username e password), in base alle istruzioni in tal senso impartite dalla Società. Tali modalità:

- ✓ consentono al segnalante di scegliere se – ed eventualmente in quale momento - rivelare o meno la propria identità;
- ✓ consentono al segnalante di dialogare con l'Organo di controllo destinatario della segnalazione, mediante invio di messaggi ed eventuali documenti dalla propria aree riservata.
- ✓ garantiscono al segnalante la completa riservatezza/anonimato, ai sensi delle previsioni normative vigenti.

La segnalazione viene, infatti, creata dal segnalante all'interno dell'area a questi riservata e perviene al RPTC e/o all'OdV, in base alla scelta effettuata, senza che venga evidenziato il mittente, a meno che il segnalante non disponga diversamente.

Nei soli casi previsti dalla normativa (cfr par. 6.5) il RPTC e/o l'OdV hanno la possibilità di risalire all'identità del segnalante, motivatamente; laddove ciò avvenisse, il soggetto segnalante è automaticamente informato di tale circostanza, visibile all'interno dell'area riservata.

In ogni caso, anche se proveniente attraverso canali differenti, viene sempre garantita la riservatezza della segnalazione.

6.4 SEGNALAZIONI ANONIME

Vengono prese in considerazione anche le segnalazioni "anonime", ossia effettuate senza identificazione del soggetto segnalante, qualora adeguatamente circostanziate, ove cioè siano in grado di far emergere fatti e situazioni relazionandoli a contesti determinati.

Sono considerate anonime le segnalazioni che:

a) sono trasmesse attraverso un canale diverso dalla piattaforma informatica (es. missiva cartacea) e che:
   - non rechino alcuna sottoscrizione da parte del segnalante;
   - rechino una sottoscrizione illeggibile o che non consenta di individuare il soggetto segnalante;
   - pur apparendo riferibili a un soggetto non consentano, comunque, di individuarlo con certezza;
b) sono trasmesse a mezzo della piattaforma informatica con la modalità "*Segnalazioni di utenti non provvisti di credenziali*".

In riferimento al punto b) si sottolinea che è possibile trasmettere una segnalazione a mezzo della piattaforma informatica, anche senza formale autenticazione, utilizzando la funzionalità "*Segnalazioni di utenti non provvisti di credenziali*". In tali ipotesi, il segnalante ha tuttavia la possibilità di inserire le proprie generalità ed i riferimenti per essere contattato. Nel caso di utilizzo della piattaforma, il segnalante "anonimo", ancorché sprovvisto di credenziali, ha comunque la facoltà di interagire con il RPCT e/o l'OdV mediante scambio di messaggi ed eventuali documenti, accedendo al Sistema con l'utilizzo di "codici di autenticazione" e "password" specifici forniti automaticamente dalla piattaforma al momento di sottomissione della segnalazione "anonima".

In ogni caso, anche se proveniente attraverso canali differenti, viene sempre garantita la riservatezza della segnalazione.

6.5 TUTELA DEL WHISTLEBLOWER

6.5.a) Tutela dell'identità del segnalante

L'identità del segnalante non può essere rivelata, come previsto dal novellato art. 54-bis del d.lgs. 165/2001, e viene protetta dagli Organi di controllo destinatari della segnalazione in ogni contesto successivo alla segnalazione, salvo i casi in cui, in seguito a disposizioni di legge speciale, l'anonimato non possa essere opposto (ad es. in caso di indagini penali, tributarie o amministrative, ispezioni, ecc.). In particolare:

- nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale;
- nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

Inoltre, in caso di procedimento disciplinare, l'identità del segnalante non può essere rivelata ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa; l'identità del segnalante potrà essere rivelata soltanto laddove:

➔ la contestazione sia fondata, in tutto o in parte, sulla segnalazione stessa e la conoscenza dell'identità del segnalante sia assolutamente indispensabile per la difesa dell'incolpato; e

➔ vi sia il consenso del segnalante.

La tutela del segnalante non è garantita in caso in cui sia accertata, anche in primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o altri reati commessi con la segnalazione ovvero in caso di responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave, come espressamente previsto dal citato art. 54-bis.

Parallelamente, sono previste nel Sistema Disciplinare di Consip specifiche sanzioni (i) per chi viola le misure di tutela del segnalante; (ii) per il segnalante interno che effettuata con dolo o colpa grave segnalazioni che si rivelano poi infondate.

6.5.b) Divieto di discriminazione

Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile[37], il soggetto tutelato (dipendente o collaboratore), che, nell'interesse dell'integrità della Società/pubblica amministrazione, effettua una segnalazione al RPCT o all'ANAC o denuncia all'Autorità giudiziaria ordinaria o a quella contabile, condotte illecite di cui sia venuto a conoscenza in ragione del proprio rapporto di lavoro, non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione (misure ritorsive o discriminatorie).

L'adozione di misure ritenute ritorsive/discriminatorie nei confronti del segnalante è comunicata all'ANAC[38] e/o all'Ispettorato nazionale del lavoro da parte dell'interessato o delle organizzazioni sindacali maggiormente rappresentative in Consip.

In ogni caso, il soggetto che ritiene di essere sottoposto a comportamenti discriminatori per il fatto di aver effettuato una segnalazione di illecito:

- ✓ può dare notizia circostanziata dell'avvenuta discriminazione al RPCT e/o all'OdV, il quale valuta la sussistenza degli elementi per effettuare agli organi/strutture competenti la segnalazione di quanto accaduto, per le eventuali azioni di competenza;
- ✓ può darne notizia al capo gerarchico del dipendente che ha operato la discriminazione, e/o al proprio capo gerarchico e/o alla Divisione Risorse Umane e Comunicazione, affinché valutino l'opportunità/necessità di adottare atti o provvedimenti opportuni;
- ✓ può dare notizia dell'avvenuta discriminazione all'organizzazione sindacale alla quale aderisce, per le azioni di competenza.

Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli. In particolare, il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo e sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante. E' onere della Società, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

---

[37]Le tutele di cui al presente paragrafo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 dell'art. 54-bis del d.lgs. 165/2001 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

[38]Art. 54-bis, comma 6, del d.lgs. 165/2001: "*Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro. Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione*."

6.5.c) Sottrazione al diritto di accesso

La segnalazione è sottratta all'accesso civico generalizzato di cui agli artt. 5 e 5-*bis* del d.lgs. 33/2013 e all'accesso previsto dagli articoli 22 e seguenti della L. 241/1990, e successive modificazioni. In generale, dunque, la segnalazione non può essere oggetto di visione né di estrazione di copia da parte di richiedenti, ricadendo nell'ambito delle ipotesi di esclusione di cui all'art. 24, c. 1, lett. a), L. 241/1990.

6.5.d) Distacco o casi analoghi

In caso di distacco del dipendente (o situazioni analoghe), questi può riferire anche di fatti accaduti in un ente diverso da quello in cui presta servizio al momento della segnalazione. In tale ipotesi, il RPCT/OdV della Società che riceve la segnalazione valuta l'inoltro all'ente cui i fatti si riferiscono, secondo criteri e modalità da quest'ultima stabilite, o, se del caso, all'ANAC.

CAPITOLO 7

MONITORAGGIO E CONTROLLI

7.1 PIANO INTEGRATO DEI CONTROLLI

L'OdV, come sopra già accennato, ha il compito di vigilare sull'effettiva e concreta applicazione/attuazione del Modello per prevenire la commissione dei reati di cui al Decreto, verificando la congruità dei comportamenti all'interno della Società rispetto allo stesso;

A tal fine, come meglio evidenziato nel cap. 5, all'OdV sono assegnati idonei e congrui poteri per lo svolgimento dell'incarico con autonomia ed effettività, ivi inclusi i poteri di vigilanza sull'attuazione effettiva delle misure previste nel Modello; devono, dunque, essere garantiti all'OdV i seguenti poteri:

- effettuare controlli sulle procedure e sui processi aziendali che abbiano impatto in materia di prevenzione dei reati presupposto, proponendo le modifiche ritenute necessarie e, nel caso di mancata attuazione, segnalare il tutto al Consiglio di Amministrazione;
- collaborare con le strutture aziendali competenti alla redazione delle procedure aziendali che abbiano impatto in materia di anticorruzione e trasparenza;
- interfacciarsi con il CdA, il Collegio sindacale, il RPCT, il DPO, il GSOS, il Dirigente preposto alla redazione dei documenti contabili societari e ciascun Referente aziendale, ai fini dell'eventuale attivazione delle azioni necessarie per il miglior espletamento dei propri compiti.

Per l'espletamento dei propri compiti, l'OdV dispone, inoltre, della libertà di accesso senza limitazioni alle informazioni aziendali rilevanti per le proprie attività di indagine, analisi e controllo; può richiedere le informazioni necessarie allo svolgimento delle attività di competenza a qualunque funzione aziendale, che è tenuta a rispondere.

Nell'implementazione delle politiche di prevenzione e per lo svolgimento dei compiti di vigilanza e controllo, l'OdV si avvale del supporto della Divisione Compliance e Societario e della Divisione Internal Audit, come meglio specificato nel proseguo. Nell'ambito dell'attività di monitoraggio l'OdV si può avvalere del supporto dei Referenti per, ciascuno per quanto di rispettiva competenza; ove lo ritenga necessario, l'OdV può avvalersi, informato il relativo Referente, anche della collaborazione degli addetti della struttura aziendale di riferimento per attività tecniche di verifica, oltre che del supporto motivato di consulenti esterni, nell'ambito delle risorse assegnate dalla Società.

Le attività di controllo sono condotte in un'ottica di integrazione e di coordinamento con gli altri organi di controllo. Pertanto l'OdV, con il supporto del responsabile della Divisione Internal Audit, definisce annualmente un Piano dei Controlli ex d.lgs. 231/01, tenendo in considerazione quanto segue:

- i risultati del risk assessment integrato condotto;
- gli interventi di *audit* svolti dalla Divisione Internal Audit nel corso del triennio precedente;
- i controlli effettuati dal RPCT nel triennio precedente;

- il Piano annuale di Audit elaborato dalla relativa Divisione;
- i follow-up degli interventi di audit;
- il Piano dei controlli dell'OdV ex d.lgs. 231/01;
- i controlli effettuati dal Dirigente preposto ai sensi della L. 262/2005, i cui risultati sono condivisi con il RPCT;
- i controlli effettati dagli altri organi di controllo;
- i Piani di azione di cui al PTPC;
- gli obblighi in tema di trasparenza;
- lo stato di attuazione delle misure preventive.

Il Piano dei Controlli ex d.lgs 231/01 è condiviso con la Divisione Internal Audit ai fini della predisposizione del Piano Integrato dei Controlli e della gestione dello stesso, onde consentire lo sfruttamento delle sinergie attraverso l'integrazione e la razionalizzazione dei controlli aziendali. Tale Piano viene infatti definito in base a: (i) Piano dei controlli del RPCT; (ii) Piano dei controlli dell'OdV; (iii) Piano di Audit della Divisione IA; (iv) Piano dei controlli del DPO; (v) Piano dei controlli in tema di sicurezza sui luoghi di lavoro. Le attività vengono effettuate dalla Divisione Internal Audit, anche con il supporto delle risorse della Divisione Compliance e Societario, laddove necessario.

Il Piano Integrato dei Controlli viene condiviso con la DCS, l'OdV, il DPO e il RPCT e successivamente sottoposto al Consiglio di Amministrazione per la relativa approvazione, entro il primo trimestre di ciascun anno.

In caso sia necessario apportare variazioni significative al Piano Integrato dei Controlli approvato – per criticità che possono emergere in corso d'anno e/o per richieste specifiche dei vertici della Società – il Piano aggiornato deve essere nuovamente sottoposto al Consiglio di Amministrazione per l'approvazione, come sopra specificato.

Il Responsabile della Divisione IA invia alla DCS, RPCT, al DPO e all'OdV le risultanze dei singoli interventi di audit, delle verifiche e il follow up delle eventuali azioni correttive suggerite. Le risultanze dei singoli controlli di cui al Piano del Controlli, in caso di necessità, sono oggetto di tempestiva segnalazione agli organi interni competenti.

7.2 ATTIVITÀ ISTRUTTORIA SULLE SEGNALAZIONI

L'OdV e/o il RPCT a seconda della competenza, in tutti i casi in cui hanno conoscenza di una violazione del Modello, del Codice etico o del PTPC, per effetto di una segnalazione o di un accertamento durante lo svolgimento delle attività di propria competenza, svolgono un'attività istruttoria sui contenuti delle segnalazioni ricevute, al termine della quale formulano le proprie valutazioni e conclusioni. Tale istruttoria non si configura in alcun caso come procedimento disciplinare ai sensi del CCNL di riferimento. Nello specifico:

- il RPCT/OdV, ricevuta la segnalazione, anche in forma anonima, la prende in carico e/o la condivide o riassegna[39] tempestivamente all'OdV/RPCT, laddove competente, al fine di verificare se sia sufficientemente circostanziata o contenga gli elementi necessari a poter effettuare le dovute verifiche
- in caso positivo, l'OdV e/o il RPCT avviano l'attività istruttoria, che può comportare (i) la richiesta di documentazione/informazioni alla struttura/Società; (ii) la richiesta di ulteriori informazioni al segnalante; (iii) l'audizione delle risorse coinvolte
- la struttura/Società deve fornire un tempestivo riscontro, comunque entro e non oltre 30 gg dalla richiesta avanzata dal RPCT e/o dall'OdV, salvo adeguata motivazione del mancato rispetto di detto termine
- l'OdV e/o il RPCT, ricevuta la documentazione/informazioni richieste, procede alla disamina delle stesse; gli Organismi posso richiedere documentazione/informazioni integrative alla struttura, che deve fornire un riscontro entro e non oltre 30 gg da quest'ultima richiesta;
- l'OdV e/o il RPCT comunicano lo stato dell'istruttoria (archiviazione - istruttoria in corso – istruttoria conclusa) al segnalante, laddove da questi richiesto. In caso di segnalazione effettuata tramite piattaforma, il segnalante può visionare lo stato in ogni momento (non letta - letta - in lavorazione - archiviata).

L'OdV e/o Il RPCT provvedono all'archiviazione delle segnalazioni, oltre che nel caso di segnalazione "anonima" non adeguatamente circostanziata, anche nei seguenti casi:

a) infondatezza della segnalazione;
b) contenuto generico;
c) incompetenza dell'OdV e/o del RPCT;
d) questioni di carattere prevalentemente personale del segnalante tese ad ottenere l'accertamento nel merito di proprie vicende soggettive.

L'OdV e/o il RPCT, a seconda della competenza, qualora, al termine della propria istruttoria o di un accertamento durante lo svolgimento delle attività di propria competenza, riscontrino una violazione del Modello, del Codice etico e/o del PTPC, ivi inclusi gli obblighi di pubblicazione, la comunicano tempestivamente, in relazione alla gravità:

violazione ascrivibile a dipendenti / dirigenti	*violazione ascrivibile ad altri destinatari*
✓ alla Divisione Risorse Umane e Comunicazione e all'Amministratore Delegato, ai fini dell'avvio del procedimento disciplinare nei confronti dei dipendenti/dirigenti	✓ alla Divisione Affari Legali e all'Amministratore Delegato / CdA, a seconda dei limiti della delega conferita all'AD, ai fini dell'avvio delle azioni di carattere contrattuale
✓ al Consiglio di Amministrazione in casi di particolare gravità	✓ al Consiglio di Amministrazione in casi di particolare gravità

[39] Nel caso di segnalazione a mezzo di piattaforma informatica, con la condivisione sia RPCT che OdV visualizzano la segnalazione e ne condividono la gestione. In caso di riassegnazione, soltanto l'organo di controllo al quale è stata riassegnata la segnalazione, può visualizzarla e gestirla in tutti i suoi aspetti.

Nell'ipotesi di violazione ascrivibile ad uno o più membri del Consiglio di Amministrazione, del Collegio sindacale, dell'OdV o al RPCT, la segnalazione viene tempestivamente sottoposta[40] all'attenzione del "Comitato dei Presidenti", composto da:

- Presidente del Consiglio di Amministrazione o Consigliere più anziano in caso di segnalazione relativa al Presidente stesso;
- Presidente del Collegio Sindacale o Sindaco più anziano in caso di segnalazione relativa al Presidente stesso;
- Presidente dell'OdV o membro più anziano in caso di segnalazione relativa al Presidente stesso;

affinché verifichi se vi siano o meno i presupposti per avviare le attività istruttorie. Il Comitato, qualora non decida di archiviare la segnalazione per manifesta infondatezza, procederà alle opportune verifiche, avvalendosi, se del caso, della Divisione Internal Audit e della Divisione Compliance e Societario, per quanto di rispettiva competenza. All'esito delle verifiche:

- ✓ dispone l'archiviazione della segnalazione, quando risulta infondata, e ne dà immediata comunicazione all'organo di riferimento, secondo lo schema che segue;
- ✓ in caso di non archiviazione, comunica le risultanze dell'Istruttoria, con relazione scritta, all'organo di riferimento secondo lo schema che segue, per l'adozione dei necessari provvedimenti, in base a quanto previsto dalla normativa vigente, dallo statuto e dal sistema disciplinare:

Violazione ascrivibile a	*Risultanze dell'istruttoria sottoposte a:*
Amministratore	✓ Consiglio di Amministrazione ✓ Collegio Sindacale ✓ p.c. OdV/RPCT se competenti per materia
Sindaco	✓ Collegio Sindacale ✓ Consiglio di Amministrazione ✓ p.c. OdV/RPCT se competenti per materia
OdV	✓ OdV ✓ Consiglio di Amministrazione ✓ p.c. Collegio Sindacale ✓ p.c. RPCT (se competente per materia)
RPCT	✓ Consiglio di Amministrazione ✓ p.c. Collegio Sindacale ✓ c.c. OdV se competente per materia

L'OdV e il RPCT garantiscono la gestione dell'istruttoria nel rispetto delle norme di riservatezza e dei principi di garanzia dell'anonimato di cui al cap. 6.6, in particolare:

[40] Curando che non venga trasmessa al Segnalato.

- laddove necessario, separare i dati identificativi del segnalante dal contenuto della segnalazione, prevedendo l'adozione di codici sostitutivi dei dati identificativi, in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi in cui ciò sia strettamente necessario;
- nella piattaforma informatica, viene sempre garantita la riservatezza del segnalatore, mediante separazione dei dati identificativi del segnalante dal contenuto della segnalazione in modo che la segnalazione possa essere processata in modalità anonima e rendere possibile la successiva associazione della segnalazione con l'identità del segnalante nei soli casi in cui ciò sia strettamente necessario e sia previsto dalla legge;
- non permettere di risalire all'identità del segnalante se non nei casi espressamente stabiliti dalla normativa vigente (cfr cap. 6.5);
- mantenere riservato, per quanto possibile, anche in riferimento alle esigenze istruttorie, il contenuto della segnalazione durante l'intera fase di gestione della stessa.

Ogni violazione di rilievo del Modello e/o del Codice etico riscontrata dall'OdV viene riportata nella relazione semestrale di competenza. Ogni violazione del PTPC e del Codice etico riscontrata dal RPCT, viene riportata nella relazione semestrale di competenza.

Resta ovviamente inteso che l'OdV e il RPCT operano nell'ottica della più ampia collaborazione e del reciproco scambio delle informazioni in base alle reciproche competenze.

Le funzioni competenti non potranno archiviare un procedimento disciplinare per violazione del Modello, del Codice Etico, del PTPC, ovvero irrogare una sanzione disciplinare, senza aver preventivamente acquisito il parere (non vincolante) rispettivamente dell'OdV e/o del RPCT, a seconda della tipologia di violazione. Il parere sull'irrogazione della sanzione deve essere sempre espresso e motivato.

CAPITOLO 8
DIFFUSIONE ED AGGIORNAMENTO DEL MODELLO

8.1 FORMAZIONE

8.1.a) Piano di formazione integrato

Consip, consapevole del valore del momento formativo e informativo per la prevenzione del rischio di reato, opera costantemente allo scopo di garantire la conoscenza da parte del personale del contenuto del Decreto e di ogni normativa aziendale inserita nel Modello. Le finalità che la Società ritiene opportuno perseguire per mezzo della formazione, tendono, dunque, in primo luogo a creare consapevolezza sulla responsabilità e sugli obblighi definiti dalla normativa, nonché ad aumentare l'attenzione sui temi dell'etica e della legalità, quali elementi determinanti per prevenire i rischi di compimento del reato.

Le azioni di comunicazione e formazione dovranno, in particolare, riguardare - oltre ai contenuti del Codice Etico - strumenti quali i poteri autorizzativi, le linee di dipendenza gerarchica, i processi e le procedure aziendali, i flussi di informazione e tutto quanto contribuisca a dare trasparenza all'attività quotidiana ad ogni livello dell'azienda.

Consip si è dunque dotata di procedure interne finalizzate alla definizione di un "*Piano annuale della formazione*", idoneo a garantire la corretta selezione e formazione del personale, anche con riguardo alle tematiche relative all'anticorruzione, alla trasparenza, all'antiriciclaggio e alla privacy.

In tale contesto, l'OdV, il RPCT, il DPO e il GSOS, sentita la Divisione Risorse Umane e Comunicazione e con il supporto della Divisione Compliance e Societario, definiscono annualmente un "*Piano di formazione integrato*", anche sulla base della formazione erogata e/o delle esigenze emerse nel corso dell'esercizio precedente, oltre che in ragione delle risultanze dei controlli effettuati nell'ambito del Piano Integrato dei Controlli

Tale Piano viene sottoposto annualmente all'attenzione dell'Amministratore Delegato per la relativa approvazione; una volta approvato, viene trasmesso alle RSU. Il Piano è elaborato nel rispetto del budget approvato dal CdA e gestito dalla Divisione Risorse Umane e Comunicazione, che fornisce il supporto organizzativo e logistico per l'erogazione degli interventi formativi.

La Divisione Risorse Umane e Comunicazione gestisce, inoltre, le attività di individuazione del personale da inserire nei vari percorsi formativi, di sensibilizzazione e quelle di informazione del personale nei settori di interesse, sulla base dei fabbisogni individuati dal RPCT, in coordinamento con l'OdV, il DPO e il GSOS per le correlate tematiche di competenza.

Sono previste diverse tipologie di formazione, erogata da personale qualificato, da organizzarsi periodicamente in corsi d'aula o con altre soluzioni che garantiscano il riscontro dell'avvenuta formazione:

generale	➔	diretta all'analisi della normativa di riferimento - rivolta a: ✓ tutti i dipendenti ✓ i collaboratori
specifica	➔	maggiormente connessa al ruolo aziendale - rivolta a: ✓ RPCT – OdV – DPO - GSOS ✓ Membri CdA ✓ Dirigenti ✓ Referenti ✓ Focal points
tecnica	➔	attinente a tematiche tecniche specifiche, connesse a determinati incarichi o ruoli aziendali (es. membro commissione di gara o RdP).

Particolare attenzione viene prestata, infine, al monitoraggio ed alla verifica del livello di attuazione dei processi di formazione e loro efficacia, attraverso la distribuzione di questionari sottoposti all'attenzione dei soggetti destinatari della formazione stessa.

8.1.b) Discenti

L'attività di formazione riguarda tutto il personale, nonché quello somministrato (ex interinale), e dovrà essere prevista e realizzata sia al personale neo-inserito sia in occasione dell'adozione/modifiche del PTPC e/o e del Modello ex d.lgs. 231/01 e/o del Sistema Privacy e/o del Modello antiriciclaggio o di ulteriori circostanze di fatto o di diritto che ne determinino la necessità.

8.2. COMUNICAZIONE E PUBBLICAZIONE DEL MODELLO E/O DEL CODICE ETICO

Conseguentemente alla delibera di approvazione del Modello e/o del Codice Etico da parte del CdA:

(i) il Modello e/o del Codice Etico viene pubblicato, a cura della DCS, sul sito internet della Società, all'interno della sezione Società Trasparente, sotto-sezione Livello 1 "*Disposizioni generali*"

(ii) la DCS dà comunicazione della pubblicazione Modello e/o del Codice Etico a tutto il personale della Società

Ogni nuova versione del Modello e/o del Codice Etico viene pubblicata all'interno della sezione Società Trasparente con le modalità previste nella Sezione Trasparenza del PTPC e per una durata di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione; decorso tale termine il documento rimane accessibile ai sensi dell'art. 5 del d.lgs. 33/2013 (Accesso civico).

8.3 INFORMAZIONE AI SOGGETTI TERZI

Ai soggetti aventi rapporti contrattuali con Consip, in particolare fornitori, consulenti e soggetti esterni all'organizzazione d'impresa che gestiscono in regime di *outsourcing* attività appartenenti

al ciclo operativo di Consip (es. consulenti del lavoro), sono fornite da parte delle funzioni aziendali di riferimento, in coordinamento con il RPCT e con l'OdV, apposite informative sulle politiche e le procedure in vigore per l'attuazione del PTPC e del Modello ex d.lgs. 231/01, sui contenuti del Codice etico, nonché sulle conseguenze che comportamenti contrari alle previsioni aziendali o alla normativa vigente possono avere sui rapporti contrattuali. E' infatti prevista al momento dell'assunzione, la sottoscrizione da parte di ciascun neo-assunto di un apposito modulo per presa visione ed accettazione della documentazione normativa aziendale di riferimento.

Laddove possibile, devono essere inserite nei testi contrattuali di riferimento specifiche clausole dirette a disciplinare tali conseguenze, quali clausole risolutive, applicazione di penali o diritti di recesso in caso di comportamenti contrari alle norme del Codice etico e/o a protocolli definiti dal PTPC e dal Modello ex d.lgs. 231/01.

CAPITOLO 9
IL SISTEMA DISCIPLINARE

9.1 IL SISTEMA DISCIPLINARE

Consip ha adottato un proprio Sistema Disciplinare idoneo a sanzionare il mancato rispetto delle misure previste dal Modello ex d.lgs. 231/01, dal Codice etico, dal PTPC.

Il tipo e l'entità delle sanzioni sono variabili in relazione alla gravità dei comportamenti e tengono conto del principio di proporzionalità previsto dall'art. 2106 del codice civile.

Le azioni in caso di violazione, la tipologia e le modalità di applicazione delle sanzioni sono descritte nel dettaglio nel documento allegato *"Sistema Disciplinare"* (cfr. All. 4).