



PR WH 01
"WHISTLEBLOWING POLICY"
PROCEDURA SEGNALEZIONE
DI ILLECITI ALL'ORGANISMO DI VIGILANZA

SOMMARIO

1.	<u>RIFERIMENTI NORMATIVI E DEFINIZIONI</u>	4
1.1	<i>RIFERIMENTI NORMATIVI – LINEE GUIDA – PARERI DI RIFERIMENTO</i>	4
1.2.	<i>DEFINIZIONI</i>	4
1.2.1.	<i>GENERALE</i>	4
1.2.2.	<i>DEFINIZIONI SECONDO L'ART. 2 DEL D.LGS. 24/2023</i>	4
1.2.3.	<i>DEFINIZIONI SECONDO L'ART. 3 DEL D.LGS. 24/2023</i>	7
2.	<u>SINOSI DEL PROVVEDIMENTO ANALISI CRITICA DELLE NORME E INTRODUZIONE DEI COMPORTAMENTI ATTESI DALLA GOVERNANCE</u>	7
2.1.	<i>QUALI MODIFICHE NORMATIVE</i>	7
2.2.	<i>COSA PUO' ESSERE OGGETTO DI SEGNALAZIONE</i>	9
2.3.	<i>CHE COSA NON SI PUO' SEGNALARE</i>	11
2.4.	<i>A QUALI SOGGETTI GIURIDICI, TRA GLI ENTI COLLETTIVI, SI APPLICA IL DECRETO E TRA QUESTI ENTI QUALI PERSONE</i>	12
2.5.	<i>LE PERSONE A CUI SI APPLICA IL DECRETO (OGGETTO DI PROTEZIONE)</i>	13
2.6.	<i>IL "GESTORE" DELLA SEGNALAZIONE</i>	14
2.7.	<i>LA FORMA DELLA SEGNALAZIONE</i>	16
2.8.	<i>I CANALI DELLA SEGNALAZIONE</i>	16
2.8.1.	<i>I CANALI DELLA SEGNALAZIONE INTERNA</i>	16
2.8.2.	<i>I SOGGETTI CUI VA AFFIDATA LA GESTIONE DELLE SEGNALAZIONI</i>	18
2.8.3.	<i>LE ATTIVITA' CUI E' TENUTO CHI GESTISCE LE SEGNALAZIONI</i>	18
2.8.4.	<i>INFORMAZIONI DA INSERIRE SUL SITO E SULLA PAGINA DELLA PIATTAFORMA PER EVITARE ERRORI DA PARTE DEL SEGNALANTE</i>	20
2.9.	<i>CANALE ESTERNO E DIVULGAZIONE PUBBLICA</i>	21
2.10.	<i>PROTEZIONE DELLA RISERVATEZZA DELLE PERSONE SEGNALANTI</i>	22
2.11.	<i>RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI – ASPETTI GENERALI</i>	22
2.12.	<i>DIVIETO DI RITORSIONE – COSA SI INTENDE PER RITORSIONE</i>	25
2.13.	<i>LE TUTELE E LA PERDITA DELLE TUTELE</i>	26
2.14.	<i>MISURE DI SOSTEGNO AI SEGNALANTI</i>	28
2.15.	<i>SANZIONI PER LE VIOLAZIONI APPLICATE DA ANAC</i>	29
3.	<u>ADEMPIMENTI WHISTLEBLOWING DA PARTE DI CENTROFOR</u>	29
3.1.	<i>COMPITI DEL PRESIDENTE DI CENTROFOR</i>	29
3.1.1.	<i>ADEMPIMENTI PER GARANTIRE LA PROTEZIONE DEI DATI PERSONALI</i>	30
4.	<u>I COMPITI DEL GESTORE DELLA SEGNALAZIONE</u>	32
5.	<u>ISTITUZIONE DEL CANALE DI SEGNALAZIONE E MODALITA' DELLA SEGNALAZIONE</u>	34
5.1.	<i>CANALE DI SEGNALAZIONE – IN GENERALE</i>	34
5.2.	<i>CANALE DI SEGNALAZIONE PREDISPOSTI DA CENTROFOR</i>	35

5.3.	CANALE ESTERNO E DIVULGAZIONE PUBBLICA	36
<u>6.</u>	<u>ARCHIVIAZIONE DELLA DOCUMENTAZIONE</u>	36
<u>7.</u>	<u>LIMITI DELLA TUTELA – RESPONSABILITA' DEL SEGNALANTE</u>	37
<u>8.</u>	<u>DISPOSIZIONI FINALI</u>	37
<u>9.</u>	<u>PUBBLICITA'</u>	37

1. RIFERIMENTI NORMATIVI E DEFINIZIONI

1.1. RIFERIMENTI NORMATIVI – LINEE GUIDA – PARERE DI RIFERIMENTO

REG. UE 679/2016: Regolamento Europeo per la protezione dei dati personali (in sigla RGPD o GDPR General Data Protection Regulation).

D.Lgs. 231/01 o Decreto: il Decreto Legislativo 8 giugno 2001, n. 231 relativo alla "Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica" e successive modifiche e integrazioni.

DECRETO LEGISLATIVO 10 marzo 2023, n. 24: Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

LINEE GUIDA ANAC: delibera 311 del 12.07.2023.

PARERE GARANTE PRIVACY: reg. 304 del 06.07.2023.

1.2. DEFINIZIONI

1.2.1. GENERALE

Centro di formazione professionale e prevenzione infortunistica dell'edilizia: Organismo Paritetico ai sensi dell'art. 51 del Decreto Legislativo 9 aprile 2008 nr. 81, d'ora in avanti Centrofor o Organismo o Ente.

Codice Etico: adottato ai sensi del D.Lgs. n. 231/01, è un documento con cui l'Ente enuncia l'insieme dei diritti, dei doveri e delle responsabilità dell'Ente rispetto a tutti i soggetti con i quali entra in relazione per il conseguimento del proprio oggetto sociale. Il Codice Etico si propone di fissare "standards" etici di riferimento e norme comportamentali che i Destinatari del Codice stesso devono rispettare nei rapporti con l'Ente ai fini di prevenzione e repressione di condotte illecite.

Modello/MOG: Modello di organizzazione, gestione e controllo ex artt. 6 e 7 del Decreto.

O.d.V.: Organismo di Vigilanza previsto dagli artt. 6, comma 1, lettera b) e 7 del D.Lgs. 231/2001, cui è affidato il compito di vigilare sul funzionamento e sull'osservanza del Modello e di curarne l'aggiornamento.

1.2.2. DEFINIZIONI SECONDO L'ART. 2 DEL D.LGS. 24/2023

a) «violazioni»: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

- 1) *illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6);*
- 2) *condotte illecite rilevanti ai sensi del D.Lgs. 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);*

- 3) *illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;*
- 4) *atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'art. 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;*
- 5) *atti od omissioni riguardanti il mercato interno, di cui all'articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;*
- 6) *atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5);*
- b) «informazioni sulle violazioni»:** *informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'art. 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni;*
- c) «segnalazione» o «segnalare»:** *la comunicazione scritta od orale di informazioni sulle violazioni;*
- d) «segnalazione interna»:** *la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna di cui all'art. 4;*
- e) «segnalazione esterna»:** *la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'art. 7;*
- f) «divulgazione pubblica» o «divulgare pubblicamente»:** *rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone;*

- g) «persona segnalante»:** la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;
- h) «facilitatore»:** una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- i) «contesto lavorativo»:** le attività lavorative o professionali, presenti o passate, svolte nell'ambito dei rapporti di cui all'art. 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile;
- l) «persona coinvolta»:** la persona fisica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente;
- m) «ritorsione»:** qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica e che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto;
- n) «seguito»:** l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;
- o) «riscontro»:** comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione;
- p) «soggetti del settore pubblico»:** le amministrazioni pubbliche di cui all'art. 1, comma 2, del D.Lgs. 30 marzo 2001, n. 165, le autorità amministrative indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli organismi di diritto pubblico di cui all'art. 3, comma 1, lettera d), del D.Lgs. 18 aprile 2016, n. 50, i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'art. 2, comma 1, lettere m) e o), del D.Lgs. 19 agosto 2016, n. 175, anche se quotate;
- q) «soggetti del settore privato»:** soggetti, diversi da quelli rientranti nella definizione di soggetti del settore pubblico, i quali:
- 1) hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato;
 - 2) rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1);

- 3) *sono diversi dai soggetti di cui al numero 2), rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1).*

1.2.3. DEFINIZIONI SECONDO L'ART. 2 DEL D.LGS. 24/2023

- a) **persone del medesimo contesto lavorativo della persona segnalante**, *di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;*
- b) **colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica**, *che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;*
- c) **enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone**

2. SINOSI DEL PROVVEDIMENTO ANALISI CRITICA DELLE NORME E INTRODUZIONE DEI COMPORTAMENTI ATTESI DALLA GOVERNANCE

2.1 QUALI MODIFICHE NORMATIVE

In data 10 marzo 2023 è stato pubblicato sulla G.U. 63 il D.Lgs. 24/2023 (di seguito il «Decreto») emanato per recepire la Direttiva (UE) 2019/1937, Parlamento europeo e del Consiglio, 23 ottobre 2019, (di seguito la «Direttiva»), riguardante la protezione delle persone che segnalano violazioni del diritto europeo e delle disposizioni normative nazionali, vigente dal 30 marzo 2023.

Tale norma, per il settore privato, costituisce il secondo intervento legislativo adottato per disciplinare il fenomeno del cd. «*whistleblowing*» dopo quello emanato il 30 novembre 2017 con la L. 179 (G.U. 291) 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».

CENTROFOR ha adottato in data 10/07/2015 il Modello Organizzativo 231, vari protocolli preventivi e il Codice Etico; CENTROFOR ha 7 dipendenti e 1 manutentore a chiamata; CENTROFOR potrebbe rientrare come soggetto portatore di processi sensibili, e questo sarà oggetto di risk assessment, in alcune delle categorie previste negli Allegati I e II del D.Lgs. 24/2023).

Per la redazione del presente protocollo si è tenuto conto:

1. **LINEE GUIDA ANAC:** delibera 311 del 12.07.2023;
2. **PARERE GARANTE PRIVACY:** reg. 304 del 06.07.2023;

3. **CONFINDUSTRIA** NUOVA DISCIPLINA "WHISTLEBLOWING" GUIDA OPERATIVA PER GLI ENTI PRIVATI - ottobre 2023;
4. **CNDCEC** "Nuova disciplina del Whistleblowing e impatto sul D.Lgs. 231/2001" – ottobre 2023.

Il nuovo art. 6 comma 2-bis del D.Lgs. 231 rinvia in toto al nuovo decreto.

Il previgente art. 6, comma 2-bis, lett. d), D.Lgs. 231/2001 stabiliva che il Modello organizzativo dovesse prevedere *"nel sistema disciplinare adottato ai sensi del comma 2, lettera e), sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate"*.

In buona sostanza: il Modello doveva punire sia gli atti di ritorsione che le segnalazioni infondate in malafede.

Tale comma è stato sostituito **dal seguente testo**, introdotto dal D.Lgs. 24/2023: *"I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)"*.

Il nuovo art. 21, comma 2, D.Lgs. 24/2023 è decisamente più ampio sul tema, stabilendo che gli enti muniti di Modello organizzativo devono prevedere, nel sistema disciplinare del Modello medesimo, *"sanzioni nei confronti di coloro che accertano essere responsabili degli illeciti di cui al comma 1"*.

In definitiva, tutti gli illeciti ai quali l'ANAC può applicare sanzioni amministrative (comma 1) devono trovare apposita sanzione anche nel Modello organizzativo.

Ebbene, il comma 1 non prevede soltanto la commissione di atti ritorsivi nei confronti del segnalante ma anche:

1. mancata istituzione di canali di segnalazione;
2. mancata adozione di procedure per l'effettuazione e la gestione delle segnalazioni;
3. adozione di procedure non conformi a quelle previste;
4. condotte di ostacolo alla segnalazione;
5. violazioni dell'obbligo di riservatezza della segnalazione;
6. omessa attività di verifica e analisi delle segnalazioni ricevute.

Non c'è dubbio che il sistema di WB debba essere presidiato da sanzioni nell'ambito del Modello.

In particolare, è senz'altro necessario prevedere nel Modello sanzioni "ad ampio spettro" per condotte con le quali il management ostacola la segnalazione o apprende o rivela indebitamente l'identità del segnalante o pone in essere condotte di retaliation nei suoi confronti.

Precisamente DEVONO ESSERE SANZIONATI:

1. atti ritorsivi nei confronti del segnalante (quindi successivi alla segnalazione e da essa dipendenti: cfr. art. 17 che contiene un elenco esemplificativo di condotte di retaliation);
2. condotte di ostacolo alla segnalazione (quindi precedenti o concomitanti rispetto ad essa: si pensi alla minaccia di licenziamento nei confronti di un dipendente che abbia manifestato l'intenzione di effettuare una segnalazione);
3. violazioni dell'obbligo di riservatezza sulla segnalazione (ex art. 12);
4. omessa attività di verifica e analisi delle segnalazioni ricevute (da parte del soggetto deputato alla loro ricezione e gestione: cfr. artt. 4 e 5) nei sette giorni per presa in carico e con risposta nei tre mesi.

Dovevano essere già previste, invece, sanzioni nel modello organizzativo per le altre ipotesi, pure previste dall'art. 21 comma 1:

1. mancata istituzione di canali di segnalazione;
2. mancata adozione di procedure per l'effettuazione e la gestione delle segnalazioni (come richiesto dall'art. 5);
3. adozione di procedure non conformi a quelle previste (sempre dall'art. 5).

Si tratta di ipotesi in cui ci troveremmo di fronte ad un Modello organizzativo già in astratto non idoneo. Si tratta, invece, di mancanze rilevabili e sindacabili dall'ANAC con possibile applicazione di sanzione amministrativa, appunto ai sensi del comma 1.

Infine, c'è da evidenziare che il rinvio agli illeciti del comma 1 impone la previsione di sanzioni nel Modello anche "nel caso di cui all'art. 16, comma 3".

Quest'ultima disposizione esclude la protezione del segnalante e sancisce l'applicazione a suo carico di una sanzione disciplinare *"quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave"*.

La presente procedura costituisce istruzione operativa per CENTROFOR per rendere compliance il Modello; saranno modificate le parti del Modello e del Codice Etico richiamate (anche con riferimento alla presente procedura). Particolare attenzione verrà data alle interferenze con la normativa privacy.

2.2. COSA PUO' ESSERE OGGETTO DI SEGNALAZIONE

L'art. 1 del Decreto, definisce l'ambito di applicazione dal punto di vista **«oggettivo»**, vale a dire: **cosa può essere «oggetto» di segnalazione**. Il Decreto chiarisce che per violazioni, si debbano intendere tutti quei *«comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato»* ed a tal fine fornisce una elencazione composta

da **due macrocategorie più una terza residuale** collegata alla farragginosa elencazione presente nell'Allegato al Decreto:

- a) La macrocategoria riguardante tutti gli illeciti amministrativi, contabili, civili o penali (diversi da quelli richiamati nelle singole disposizioni normative dell'Allegato);
- b) La macrocategoria riguardante la «231» suddivisa, com'era avvenuto nel novembre del 2017, tra:
 - I. condotte illecite «rilevanti» ai sensi del D.Lgs. 231/2001. Da intendersi quale richiamo alle singole fattispecie di reato in esso espressamente menzionate (elencazione tassativa);
 - II. violazioni dei modelli; vale a dire violazioni che riguardano le regole scritte nel Modello – tipicamente nella Parte Speciale dello stesso o nel Codice Etico.
- c) La terza categoria relativa ai n. 3), 4), 5) e 6), lett. a), riguarda gli illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'Allegato al Decreto; atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'art. 325, Trattato sul funzionamento dell'Unione europea; o atti od omissioni riguardanti il mercato interno di cui all'art. 26, par. 2, Trattato. Quest'ultima categoria appare come quella maggiormente orientata a tutelare interessi di carattere pubblico.

Dalla lettura del dettato normativo emerge che l'ambito oggettivo del Decreto è la «tutela del segnalante», che viene riconosciuta dalla norma **non per qualsiasi segnalazione, bensì solo per quelle che riguardano «violazioni» a:**

- a. disposizioni normative nazionali;
- b. disposizioni normative dell'Unione Europea.

Vi sono **due limitazioni:**

- la prima, prevede che saranno prese in considerazione **solo le «violazioni» che «ledono l'interesse pubblico» o «l'integrità» della «amministrazione pubblica» o «dell'ente privato»;**
- la seconda limitazione inserita nel comma 1 stabilisce che si deve trattare di violazioni di cui il **segnalante sia venuto a conoscenza «in un contesto lavorativo»** (sia pubblico che privato); sono escluse dall'ambito oggettivo tutte quelle violazioni che siano state conosciute o riscontrate accidentalmente al di fuori del contesto lavorativo o per *relata refero* da parte di soggetti ricompresi nel contesto lavorativo, ma che le abbiamo rivelate a soggetti esterni. **Costoro, stante il dettato normativo, non sono legittimati a formulare la segnalazione e, anche se effettuino la segnalazione, non usufruiscono delle tutele accordate dal Decreto ai segnalanti** (anche se saranno comunque destinatari delle comunicazioni di cui oltre); la segnalazione dovrà comunque essere oggetto di valutazione.

Il legislatore ha **tipizzato gli illeciti, gli atti, i comportamenti o le omissioni che possono essere segnalati**, indicando in modo dettagliato – anche se piuttosto complesso – che cosa è qualificabile come violazione.

Le segnalazioni possono riguardare:

- a. violazioni di norme nazionali e di norme dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'ente;
- b. violazioni commesse;
- c. violazioni non ancora commesse, ma che il segnalante ritiene possano esserlo sulla base di elementi concreti (fondati sospetti);
- d. condotte volte ad occultare le violazioni;
- e. violazioni intervenute nell'ambito di un rapporto di lavoro nel frattempo terminato;
- f. violazioni intervenute nel periodo di prova;
- g. violazioni intervenute nel periodo in cui il rapporto di lavoro non è ancora iniziato, qualora le informazioni sulle violazioni oggetto della segnalazione siano state acquisite durante il processo di selezione o in altre fasi precontrattuali.

2.3. CHE COSA NON SI PUO' SEGNALARE

Il Decreto **non trova applicazione** nei confronti delle:

- a. segnalazioni che riguardano *«contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante ... che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate»*.
- b. Segnalazioni che sono **già previste come obbligatorie da altre normative specifiche**, come ad es. quella prevista dall'art. 8, D.Lgs. 58/1998, (Testo Unico in materia di intermediari finanziari) secondo cui *«il collegio sindacale informa senza indugio la Banca d'Italia e la CONSOB di tutti gli atti o i fatti, di cui venga a conoscenza nell'esercizio dei propri compiti, che possano costituire un'irregolarità nella gestione ovvero una violazione delle norme che disciplinano l'attività delle SIM, delle società di gestione di risparmio, delle Sicav o della Sicaf»*.
- c. Segnalazioni che riguardano la sicurezza nazionale e la difesa.
- d. I commi 3 e 4, art. 1, completano il quadro degli **ambiti sottratti all'applicabilità del Decreto, tra cui: il segreto professionale (forense e medico), i segreti di Stato, le disposizioni di procedura penale, l'autonomia e indipendenza della magistratura, la difesa nazionale, la pubblica sicurezza, il diritto dei lavoratori di consultare i sindacati di appartenenza.**

Resta ferma la normativa in materia di: i) informazioni classificate; ii) segreto medico e forense; iii) segretezza delle deliberazioni degli organi giurisdizionali; iv) norme di procedura penale sull'obbligo di segretezza delle indagini; v) disposizioni sull'autonomia e indipendenza della magistratura; vi) difesa nazionale e di ordine e sicurezza pubblica; vii) esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati.

2.4. A QUALI SOGGETTI GIURIDICI, TRA GLI ENTI COLLETTIVI, SI APPLICA IL DECRETO E TRA QUESTI ENTI QUALI PERSONE

Dopo l'art. 2 dedicato alle «definizioni», il Decreto presenta l'art. 3 che delimita l'ambito di applicazione soggettivo della norma. Vale a dire, a quali soggetti giuridici, tra gli enti collettivi, si applica il Decreto e – tra questi enti – a quali persone.

Per comprendere a quali enti collettivi si applica il Decreto in commento dobbiamo far riferimento alle due definizioni contenute nell'art. 2, lett. p) e q).

A) ENTI DEL «SETTORE PUBBLICO», OMISSIS...:

B) ENTI DEL «SETTORE PRIVATO»

Tale categoria viene identificata facendo riferimento alle **definizioni contenute nell'art. 2 (lett. q)** e risulta suddivisa nei seguenti tre sottogruppi:

1. gli enti che hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato;
2. gli enti che rientrano nell'ambito di applicazione delle disposizioni normative elencate nell'Allegato al Decreto, anche se nell'ultimo anno non hanno raggiunto il numero di cinquanta lavoratori¹;
3. gli enti che hanno adottato un Modello di organizzazione, gestione e controllo ai sensi del D.Lgs. 231/2001, anche se nell'ultimo anno non hanno raggiunto il numero di 50 lavoratori.

¹ L'Allegato al Decreto è suddiviso in due parti (Parte I e II) e ciascuna Parte è contraddistinta da lettere capitali. Per facilitare la lettura le riportiamo secondo la seguente schematizzazione semplificata:

Parte I:

- A. Appalti pubblici;
 - B. Mercati finanziari, prevenzione del riciclaggio e del terrorismo;
 - C. Sicurezza e conformità dei prodotti;
 - D. Sicurezza dei trasporti;
 - E. Tutela dell'ambiente;
 - F. Radioprotezione e sicurezza nucleare;
 - G. Sicurezza degli alimenti e dei mangimi, salute e benessere degli animali;
 - H. Salute pubblica;
 - I. Protezione dei consumatori;
 - J. Tutela della vita privata e dei dati personali e sicurezza delle reti e dei sistemi informativi
- Parte II
- A. Servizi prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo;
 - B. Sicurezza dei trasporti;
 - C. Tutela dell'ambiente.
- o di dipendenti al 31.12.2022 e così via

Con riguardo alla prima categoria sub 1) – gli enti privati con almeno 50 lavoratori – e sub 2) – enti che pur avendo meno di 50 dipendenti operano negli ambiti previsti dalla Direttiva – se non hanno adottato un Modello 231, è obbligatorio implementare un sistema di whistleblowing così come previsto dal Decreto per segnalare le violazioni alle normative del diritto UE, attraverso tutti e tre i canali di segnalazione (interno, esterno o tramite divulgazione pubblica). Laddove sia stato adottato un Modello 231 il sistema di whistleblowing dovrà consentire anche le segnalazioni delle violazioni del Modello.

Per gli enti privati che non raggiungono la soglia dei 50 lavoratori non è obbligatorio il sistema di whistleblowing ed il Modello rimane facoltativo, ma qualora adottato (sub 3) il sistema dovrà consentire segnalazioni attinenti ai reati previsti dal D.Lgs. 231/2001 o a violazioni del Modello, nel rispetto del nuovo Decreto. **In tal caso, la segnalazione può essere effettuata soltanto attraverso il canale interno che deve essere predisposto in linea con le garanzie, le tutele e il regime sanzionatorio previsti dal Decreto.** In conclusione, con il Decreto in esame si estende l'ambito di applicazione della disciplina sul whistleblowing anche agli enti con più di 50 lavoratori, o con meno di 50 lavoratori se operano in determinati settori rilevanti per l'Unione, i quali non hanno adottato un «Modello 231».

I destinatari della normativa sono individuati dall'art. 3 del decreto legislativo citato, in particolare per quanto concerne il settore privato l'obbligo è esteso anche alle imprese che non abbiano adottato il modello di gestione dei rischi di cui al D.Lgs. n. 231 del 2001, ma che versino in una delle seguenti ipotesi:

- abbiano impiegato nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato²;
- o che si occupino di alcuni specifici settori (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente), anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato.

2.5. LE PERSONE A CUI SI APPLICA IL DECRETO (OGGETTO DI PROTEZIONE)

Per comprendere l' **"ambito soggettivo"** si deve far riferimento ai commi 3 e 4, dell'art. 3, che riporta la seguente elencazione di soggetti così suddivisi (si riporta l'elencazione completa anche se i punti a) e b) riguardano il settore pubblico, escluso dalla presente trattazione):

- a. i dipendenti delle pubbliche amministrazioni, trattati separatamente in ragione della peculiarità del rapporto di lavoro pubblico (D.Lgs. 165/2001, art. 1, comma 2);
- b. i dipendenti di tutti gli altri enti del «settore pubblico»;
- c. i lavoratori subordinati del «settore privato» (incluse le prestazioni occasionali);

² Quindi per il 2023 si farà riferimento al numero medio di dipendenti al 31.12.2022 e così via.

- d. i lavoratori autonomi (inclusi i rapporti di collaborazione di cui all'art. 409 c.p.c., es.: gli Agenti di commercio o i rapporti di collaborazione che si concretizzano in una prestazione di opera continuativa e coordinata anche se non a carattere subordinato);
- e. i lavoratori o collaboratori, che svolgono la propria attività lavorativa presso enti «fornitori» di beni, servizi e lavori agli enti del settore pubblico o privato;
- f. i liberi professionisti e i consulenti degli enti privati o pubblici;
- g. i volontari e i tirocinanti (anche non retribuiti);
- h. gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche di fatto.

L'art. 3 chiarisce che la tutela accordata dal Decreto, sotto il profilo soggettivo, deve **intendersi riconosciuta anche quando il rapporto di lavoro (*rectius*: il rapporto «giuridico») non sia formalmente sussistente**. Vale a dire anche nei seguenti casi:

- quando il rapporto non è ancora iniziato (ad es.: nella fase di selezione o di recruiting);
- durante il periodo di prova;
- successivamente allo scioglimento del rapporto, (ma sempre per fatti appresi durante il rapporto di lavoro).

Infine, l'art. 3 presenta un ultimo novero di soggetti a cui il legislatore intende estendere le tutele previste dal Decreto, composto dai seguenti soggetti:

- a) i «*facilitatori*». L'art. 2, lett. h), chiarisce che è un facilitatore «una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo». La norma, poi, chiarisce che l'assistenza deve essere mantenuta riservata.
- b) Le persone appartenenti al «medesimo contesto lavorativo» del segnalante, che *hanno con costui un rapporto di parentela entro il quarto grado³ o uno «stabile legame affettivo»*.
- c) I «colleghi di lavoro» che hanno con il segnalante un «rapporto abituale o corrente».
- d) «gli enti di proprietà della persona segnalante» e le persone che in essi operano.

2.6. IL GESTORE DELLA SEGNALAZIONE

L'articolo, poi, stabilisce che la «gestione» del canale di segnalazione è affidata:

- ad un «ufficio interno», «autonomo e dedicato» e con «personale specificatamente formato» per la gestione del canale; ovvero
- ad un «soggetto esterno», anch'esso autonomo e con personale specificatamente formato.

Queste le caratteristiche:

³ (i gradi di parentela si calcolano contando ciascun passaggio risalendo fino al capostipite comune e poi riscendendo, meno il capostipite comune. Per cui due cugini sono parenti di 3° grado - dal figlio, al padre, poi al nonno, poi allo zio, fino al nipote = sono 4 passaggi - 1 = 3°)

- deve essere nominato dall'Organo dirigente ossia l'organo che a seconda della struttura di governance adottata, rappresenti il vertice dell'Organismo (il C.d.A.);
- deve essere autonomo e dedicato alla gestione delle segnalazioni;
- deve essere specificatamente formato;
- deve essere remunerato;
- deve essere definito un suo Regolamento (compiti, poteri, autonomia, revoca);
- deve essere dotato di risorse (per l'espletamento delle attività di indagine: può avvalersi di soggetti specializzati nella gestione di determinate tipologie di indagini);
- è passibile di responsabilità ivi incluso il rischio di applicazioni di sanzioni ad personam (art. 21 «sanzioni», comma 1, lett. b): da 10.000 a 50.000 euro quando si accerta che «non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute»).

CENTROFOR intende esternalizzare la gestione di ogni tipo di segnalazione, sia in relazione alle violazioni 231, sia in relazione alle altre violazioni sopra menzionate; l'incarico verrà affidato all'O.d.V. Monocratico (soggetto che possiede il requisito dell'autonomia, che, ad avviso di ANAC, va declinato come imparzialità e indipendenza).

Si segnala fin d'ora che la gestione del canale di Whistleblowing da parte dell'Organismo di Vigilanza consisterà in un **mero apporto di verifica procedimentale**, con eventuali raccomandazioni per la Governance interna di riferimento (attività, queste ultime, la prima doverosa da parte dell'Organismo e la seconda compatibile con il suo ruolo). Nell'ambito del mandato di vigilanza e del relativo budget O.d.V. è chiamato a vigilare e nell'ambito di tali attività rientra anche l'attività di verifica direttamente con investigazioni interne riguardanti specifici fatti/comportamenti e la formulazione di raccomandazioni per fare adottare da parte dei vertici dell'ente misure e provvedimenti organizzativi atti a fronteggiare la situazione segnalata (**escludendosi che vi sia in detta attività ingerenza alcuna nelle attività tipicamente gestoria, che rimangono di esclusiva competenza dell'ente - attività tipicamente "gestorie"**).

Non spetta al soggetto preposto alla gestione della segnalazione accertare le responsabilità individuali qualunque natura esse abbiano, né svolgere controlli di legittimità o di merito su atti e provvedimenti adottati dall'ente/amministrazione oggetto di segnalazione, a pena di sconfinare nelle competenze dei soggetti a ciò preposti all'interno di ogni ente o amministrazione ovvero della magistratura; né al gestore spetta l'apertura di procedimenti disciplinari e l'applicazione di sanzioni. **Al gestore del canale non spetta il compito di intraprendere azioni rimediali o sanzionatorie.**

2.7. LA FORMA DELLA SEGNALAZIONE

L'art. 4, poi, prosegue chiarendo che le segnalazioni possono essere effettuate in forma «scritta» o «orale». Il comma poi aggiunge che la segnalazione può avvenire anche mediante «un incontro» «diretto».

Quanto alle segnalazioni anonime il Decreto è chiaramente pensato per soggetti segnalanti che si palesano e ciò lo si evince dal requisito della tutela della riservatezza e dal sistema di tutele per il segnalante. Tuttavia il fatto che il Decreto non le abbia espressamente regolamentate non significa che non possano essere inviate e, sicuramente, non giustificerebbe la scelta estrema di vietarle.

Le segnalazioni anonime verranno prese pertanto in considerazione nei soli casi in cui le stesse siano ben circostanziate e fondate su elementi di fatto precisi e concordanti, così come era previsto sotto la previgente norma sul whistleblowing (L. 179/2017).

È chiaro che la scelta implica, da un punto di vista squisitamente giuridico, la non applicabilità degli obblighi di «dare seguito» né tantomeno quello di «dare riscontro» a dette segnalazioni e dei relativi termini previsti dal Decreto (7 giorni, 3 mesi), fatta salva l'ipotesi che l'anonimo segnalante venga successivamente identificato. Idem dicasi per gli obblighi di riservatezza, che all'evidenza non possono trovare applicazione neppure indiretta.

2.8. I CANALI DELLA SEGNALAZIONE

Devono essere istituiti i seguenti canali di segnalazione, che si dovranno occupare della gestione della stessa:

1. interno nell'ambito del contesto lavorativo o con attribuzione ad un consulente esterno;
2. esterno (ANAC); solo come richiamo esplicativo alla possibilità concreta di farvi ricorso;
3. divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
4. denuncia all'Autorità giudiziaria o contabile.

2.8.1. I CANALI DELLA SEGNALAZIONE INTERNA

L'art. 4 del Decreto, dal titolo «canali di segnalazione», dispone che i soggetti del settore pubblico **e quelli del settore privato «attivano» «propri» canali di segnalazione.**

Tali canali per la segnalazione cd. «interna» devono garantire la riservatezza dell'identità del segnalante e del segnalato, nonché del contenuto della segnalazione.

La riservatezza può essere assicurata anche tramite strumenti di crittografia. L'uso della congiunzione copulativa «anche» non impone che necessariamente la riservatezza debba essere garantita soltanto con strumenti di crittografia, ma questo chiaro riferimento ci conferma l'attesa sul livello di garanzia richiesto dal legislatore.

La norma, poi, per come è stata varata implica che i modelli ex D.Lgs. 231/2001 devono «prevedere» l'esistenza ed il funzionamento di detti canali quale requisito di idoneità del modello stesso. In altre parole, i canali di comunicazione interna costituiscono elementi fondamentali del Modello 231 e, pertanto, su di essi andrà a ricadere la valutazione di idoneità che il giudice è chiamato a svolgere ai fini del riconoscimento dell'esimente prevista da D.Lgs. 231/2001.

L'uso del plurale («attivano propri canali»), come nel 2017, chiarisce che i canali di segnalazione devono essere più di uno.

CENTROFOR adotterà quindi due canali di segnalazione per ogni categoria di segnalazione (231 e diverse da 231).

L'intento del legislatore, come sopra anticipato, è quello di incoraggiare le persone segnalanti a rivolgersi, innanzitutto, all'ente a cui sono "collegati".

I soggetti del settore privato cui si applica il D.Lgs. n. 24/2023, **sentite le rappresentanze o le organizzazioni sindacali** (ai sensi dell'art. 51, D.Lgs. n. 81/2015, si tratta delle organizzazioni sindacali comparativamente più rappresentative sul piano nazionale, delle rappresentanze sindacali aziendali di queste ultime ovvero dalla rappresentanza sindacale unitaria), definiscono in un apposito atto organizzativo le procedure per il ricevimento delle segnalazioni e per la loro gestione, predisponendo e attivando al proprio interno appositi canali di segnalazione.

Verrà mantenuto il canale cartaceo; modificato secondo le Linee Guida ANAC; verrà introdotta la possibilità di segnalazione attraverso uso di strumento informatico accessibile solo al gestore, specificamente formato ed informato sull'uso delle stesse; quanto al canale "orale" verrà introdotta la possibilità di richiedere l'audizione, specificando che l'audizione verrà registrata e verrà redatto verbale sintetico.

Nell'atto organizzativo, adottato dall'organo di indirizzo, è opportuno che almeno vengano definiti:

- il ruolo e i compiti dei diversi soggetti cui è consentito l'accesso alle informazioni e ai dati contenuti nella segnalazione, limitando il trasferimento di questi ultimi ai casi strettamente necessari;
- le modalità e i termini di conservazione dei dati appropriate e proporzionate ai fini della procedura di whistleblowing.

CENTROFOR ha adottato il Modello di Organizzazione e Gestione ai sensi del D.Lgs. n. 231/2001; il presente protocollo costituisce regolazione normativa interna di adempimento (ai sensi dell'art. 6 comma 2 *bis*); costituisce altresì adempimento dell'obbligo normativo di gestione delle segnalazioni previste dall'art. 2 D.Lgs. cit..

Per essere ritenuti adeguati i canali di segnalazione interna devono:

1. garantire la riservatezza anche tramite il ricorso a strumenti di crittografia, ove siano utilizzati strumenti informatici:

- a) della persona segnalante;
- b) del facilitatore;
- c) della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- d) del contenuto della segnalazione e della relativa documentazione;

2. consentire di effettuare segnalazioni:

- a. in forma scritta, anche con modalità informatiche (mail dedicata);
- b. orale, attraverso linee telefoniche o in alternativa con sistemi di messaggistica vocale, ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

2.8.2. I SOGGETTI CHE VA AFFIDATA LA GESTIONE DELLE SEGNALAZIONI

Gli enti del settore privato nell'affidare tale incarico devono valutare se il soggetto abbia le caratteristiche indispensabili per svolgere l'attività richiesta.

In particolare, i soggetti che gestiscono le segnalazioni devono:

- a. essere **autorizzati al trattamento dei dati personali da parte degli enti** e quindi essere destinatari di una specifica formazione in materia di privacy e di audit (sul punto si veda oltre);
- b. essere **nominati Responsabili del trattamento in base ad un accordo appositamente stipulato con l'ente;**
- c. assicurare indipendenza e imparzialità;
- d. ricevere un'adeguata formazione professionale sulla disciplina del whistleblowing, anche con riferimento a casi concreti.

I canali interni devono essere progettati in modo da consentire un accesso selettivo alle segnalazioni solo da parte del personale autorizzato.

CENTROFOR ha deciso di nominare gestore delle segnalazioni l'O.d.V. 231 che ha specifiche competenze e capacità professionali sia in materia di audit, che in materia di privacy, che in relazione alla specifica gestione delle segnalazioni Whistleblowing.

2.8.3. LE ATTIVITA' CUI E' TENUTO CHI GESTISCE LE SEGNALAZIONI

Il decreto, nell'ottica di assicurare una efficiente e tempestiva gestione della segnalazione, prevede poi un iter procedurale che va rispettato da chi gestisce le segnalazioni.

Tale soggetto infatti:

- a. rilascia al segnalante un **avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione;**
- b. mantiene le interlocuzioni con la persona segnalante;

- c. dà un corretto seguito alle segnalazioni ricevute;
- d. fornisce un **riscontro al segnalante nel termine di tre mesi**⁴. La persona segnalante va informata dell'esito della segnalazione entro il **termine di tre mesi dalla data dell'avviso di ricevimento o, in mancanza di tale avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della segnalazione.**

In particolare, un corretto seguito implica, in primo luogo, nel rispetto di tempistiche ragionevoli e della riservatezza dei dati, una valutazione sulla sussistenza dei requisiti essenziali della segnalazione per valutarne l'ammissibilità e poter quindi accordare al segnalante le tutele previste. Analizzata la segnalazione il gestore del canale può:

- a. disporre l'archiviazione per manifesta infondatezza;
- b. provvedere ad aprire indagine istruttoria documentale o testimoniale ai fini della definizione della segnalazione.

L'archiviazione, che deve essere succintamente motivata, può essere disposta per:

- a. **infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti**; il riscontro può ad esempio consistere nella comunicazione dell'archiviazione della procedura per mancanza di prove sufficienti o altri motivi, o perché riguardante una delle ipotesi previste dall'art. 1, co. 1, lett. a), b) e c) del D.L.vo 24/2023 (riportate al precedente punto 2.1).
- b. **accertato contenuto generico della segnalazione di illecito** tale da non consentire la comprensione dei fatti ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente. Ove quanto segnalato non sia adeguatamente circostanziato, chi gestisce può chiedere elementi integrativi al segnalante tramite il canale a ciò dedicato, o anche di persona, ove il segnalante abbia richiesto un incontro diretto.

Una volta **valutata l'ammissibilità della segnalazione**, come ricompresa nella normativa Whistleblowing, i soggetti cui è affidata la gestione del canale di segnalazione avviano l'istruttoria interna sui fatti o sulle condotte segnalate per valutare la sussistenza degli stessi.

All'esito dell'istruttoria, detti soggetti forniscono un riscontro alla segnalazione, dando conto delle misure previste o da adottare per dare seguito alla segnalazione e dei motivi della scelta effettuata, o disponendo l'archiviazione.

L'esito della segnalazione, con motivazione deve essere comunicata, anche per estratto, al segnalante.

⁴ Sul punto con riguardo ai requisiti per effettuare la segnalazione esterna, è venuto meno il riferimento «all'esito negativo» sostituito dal «non ha avuto esito». Grazie a questa differenza terminologica il ricorso alla segnalazione esterna oggi (nella versione definitiva del Decreto) è possibile solo qualora non vi sia stata risposta alla segnalazione e non quando a questa abbia fatto seguito una risposta negativa

2.8.4. INFORMAZIONI DA INSERIRE SUL SITO E SULLA PAGINA DELLA PIATTAFORMA PER EVITARE ERRORI DA PARTE DEL SEGNALANTE

È importante che l'Ente chiarisca a chi è interessato a presentare una segnalazione **l'opportunità di indicare chiaramente nell'oggetto della segnalazione che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni subite in ragione della segnalazione.**

Tale specificazione consente, laddove la segnalazione pervenga erroneamente ad un soggetto non competente oppure attraverso un canale diverso da quelli specificamente previsti dal decreto, la trasmissione tempestiva da parte di quest'ultimo al soggetto autorizzato a ricevere e gestire le segnalazioni di whistleblowing. Ad esempio, se una segnalazione perviene in busta chiusa sulla quale è indicato che si tratta di una segnalazione di whistleblowing, colui che la riceve, senza aprirla, la trasmette tempestivamente ai soggetti competenti.

In assenza della chiara indicazione, infatti, la segnalazione potrebbe essere trattata come ordinaria. **È necessario, quindi, che l'Ente chiarisca bene nel sito istituzionale e anche nella stessa pagina della piattaforma dedicata, quali sono le diverse conseguenze in caso di segnalazione ordinaria e di Whistleblowing.** È utile anche che, negli stessi modelli per la trasmissione delle segnalazioni ordinarie, sia chiesto ai segnalanti di precisare se intendono o meno mantenere riservata la propria identità e avvalersi delle tutele previste per il Whistleblower.

Inoltre, i soggetti che gestiscono il canale di segnalazione interno mettono a disposizione informazioni sull'utilizzo del canale interno e di quello esterno con particolare riguardo ai presupposti per effettuare le segnalazioni attraverso tali canali, sui soggetti competenti cui è affidata la gestione delle segnalazioni nonché sulle procedure.

Tutte le attività di verifica devono in ogni caso rispettare le specifiche norme di settore e limiti stabiliti dalle disposizioni in materia di controlli a distanza (art. 4 della L. 20 maggio 1970, n. 300, cui fa rinvio l'art. 114 del Codice) e di quelle che vietano al datore di lavoro di acquisire e comunque trattare informazioni e fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore o comunque afferenti alla sua sfera privata (art. 8 della L. 20 maggio 1970, n. 300 e art. 10 D.Lgs. 10 settembre 2003, n. 276, cui fa rinvio l'art. 113 del Codice).

Tali informazioni devono essere chiare e facilmente accessibili, anche, per quanto possibile, alle persone che pur non frequentando i luoghi di lavoro, siano legittimate a presentare segnalazioni di whistleblowing. Vanno esposte, per esempio, nei luoghi di lavoro in un punto visibile, accessibile a tutte suddette persone nonché in una sezione apposita del sito web istituzionale dell'ente ed essere incluse altresì nei corsi e nelle formazioni di etica e integrità.

In ogni caso, le amministrazioni e gli enti possono prevedere nei propri Codici di comportamento o codici di condotta uno specifico dovere di trasmissione immediata e tempestiva, laddove si riceva una segnalazione di whistleblowing non essendo soggetto autorizzato.

2.9. CANALE ESTERNO E DIVULGAZIONE PUBBLICA

In via prioritaria, i segnalanti sono incoraggiati a utilizzare il canale interno e, solo al ricorrere di certe condizioni, possono EFFETTUARE UNA SEGNALAZIONE ESTERNA O UNA DIVULGAZIONE PUBBLICA.

1. I segnalanti possono utilizzare il canale esterno (ANAC) quando:

- non è prevista, nell'ambito del contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna ovvero questo, anche se obbligatorio, non è attivo o, anche se attivato, non è conforme a quanto richiesto dalla legge;
- la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;
- la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione potrebbe determinare un rischio di ritorsione;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

L'ANAC deve:

- dare avviso alla persona segnalante del ricevimento della segnalazione entro 7 giorni dalla data del suo ricevimento, salvo esplicita richiesta contraria della persona segnalante ovvero salvo il caso in cui l'ANAC ritenga che l'avviso pregiudicherebbe la protezione della riservatezza dell'identità della persona segnalante;
- mantenere le interlocuzioni con la persona segnalante e richiedere a quest'ultima, se necessario, integrazioni;
- dare diligente seguito alle segnalazioni ricevute;
- svolgere l'istruttoria necessaria a dare seguito alla segnalazione, anche mediante audizioni e acquisizione di documenti;
- dare riscontro alla persona segnalante entro 3 mesi o, se ricorrono giustificate e motivate ragioni, 6 mesi dalla data di avviso di ricevimento della segnalazione esterna o, in mancanza di detto avviso, dalla scadenza dei 7 giorni dal ricevimento;
- comunicare alla persona segnalante l'esito finale della segnalazione.

Istruzioni per l'uso

- È possibile accedere all'applicazione tramite il portale dei servizi ANAC al seguente link:
<https://whistleblowing.anticorruzione.it/#/>

- Registrando la segnalazione su questo portale, si otterrà un codice identificativo univoco, "**key code**", che dovrai utilizzare per "dialogare" con Anac in modo spersonalizzato e per essere costantemente informato sullo stato di lavorazione della segnalazione inviata.

2. I segnalanti possono effettuare direttamente una **DIVULGAZIONE PUBBLICA** quando:

- la persona segnalante ha previamente effettuato una segnalazione interna ed esterna ovvero ha effettuato direttamente una segnalazione esterna e non è stato dato riscontro entro i termini stabiliti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- la persona segnalante ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa.

2.10. PROTEZIONE DELLA RISERVATEZZA DELLE PERSONE SEGNALANTI

- L'identità del segnalante **non può essere rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni**;
- la protezione riguarda non solo il nominativo del segnalante ma anche tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del segnalante;
- la segnalazione è **sottratta all'accesso agli atti amministrativi e al diritto di accesso civico generalizzato**;
- la protezione della riservatezza è estesa all'identità delle persone coinvolte e delle persone menzionate nella segnalazione fino alla conclusione dei procedimenti avviati in ragione della segnalazione, nel rispetto delle medesime garanzie previste in favore della persona segnalante.

2.11. RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI - ASPETTI GENERALI

Ai fini del rispetto della normativa in materia di protezione dei dati personali, occorre identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, **in particolare quella di titolare e di responsabile del trattamento** (art. 4, par. 1, punto 7 del Regolamento).

Il titolare, è il soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati nonché una "responsabilità generale" sui trattamenti posti in essere (v. art. 5, par. 2 c.d. "accountability" e 24 del Regolamento), anche quando questi siano effettuati da altri soggetti "per suo conto" (cons. 81, artt. 4, punto 8) e 28 del Regolamento; cfr.

anche provvedimento Garante privacy n. 81 del 7 marzo 2019, doc. web 9121890; provvedimento Garante privacy n. 160 del 17 settembre 2020, doc. web 9461168).

In CENTROFOR, titolare del trattamento privacy è l'Ente nella persona del Presidente del Cda.

Il rapporto tra titolare e responsabile deve essere regolato da un contratto o da altro atto giuridico, stipulato per iscritto che, oltre a vincolare reciprocamente le due figure, consente al titolare di impartire istruzioni al responsabile e prevede, in dettaglio, quale sia la materia disciplinata, la durata, la natura e le finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare. **Il Responsabile del trattamento è, pertanto, legittimato a trattare i dati degli interessati "soltanto su istruzione documentata del titolare"** (art. 28, par. 3, lett. a) del Regolamento).

Il trattamento di dati personali relativi al ricevimento e alla gestione delle segnalazioni è effettuato dai soggetti del settore privato, nonché da ANAC, in qualità di titolari del trattamento, nel rispetto dei principi europei e nazionali in materia di protezione di dati personali, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte nelle segnalazioni, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati. **La specifica gestione delle segnalazioni può essere attribuita a consulenti esterni che operano, stanti le condizioni più sopra riportate come Responsabili del trattamento.**

In CENTROFOR il gestore del canale è esterno, è nominato con **atto di incarico scritto che deve essere sottoscritto per accettazione; l'atto contiene le istruzioni del titolare.**

Il gestore del canale è nominato Responsabile del trattamento

L'art. 13 disciplina la protezione dei dati personali dei trattamenti dei dati personali che riguardano le segnalazioni ed estende tutele di cui al GDPR e Codice Privacy all'intero processo di segnalazione; il comma 2 dell'art. 13 precisa, altresì, che **i dati non utili alla segnalazione devono essere immediatamente cancellati** richiamando i principi di cui all'art. 5 del GDPR che impongono, tra gli altri, il rispetto dei principi di finalità e minimizzazione del trattamento. Il decreto in parola richiama il rispetto dei diritti degli interessati riconosciuti dagli artt. 15 e ss. del GDPR - i diritti di cui agli artt. da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'art. 2-*undecies* del D.Lgs. 30 giugno 2003, n. 196; tuttavia occorre tenere presente che l'art. 2 *undecies* del Codice Privacy individua delle eccezioni all'esercizio dei diritti in determinate condizioni alcune delle quali sono speculari alla tutela del segnalante.

Il titolare del trattamento è tenuto a fornire specifiche informazioni nel rispetto del principio di trasparenza e dell'art. 13 del GDPR ai segnalanti, nonché ad attuare, come anzidetto, specifiche misure di sicurezza per tutelare la riservatezza delle informazioni. Il comma 5 dell'art. 13 richiama l'importanza della data governance. Invero, risulta evidente come la delicatezza della disciplina imponga l'adozione di specifiche nomine ai soggetti che partecipano al processo siano essi interni, esterni e/o persino in situazioni di contitolarità. La governance del

processo nonché quello di corretta gestione dei soggetti che partecipano al trattamento è un elemento essenziale da cui si estrinseca, altresì, l'accountability richiesto dal GDPR. Tale necessità viene richiamata anche dall'articolo 12 del decreto in esame relativo all'obbligo di riservatezza, il quale sancisce **l'obbligo di nominare i soggetti che partecipano al processo nel rispetto del combinato disposto di cui all'art. 29 e 32 del GDPR nonché nel dell'art. 2 quaterdecies del Codice privacy.**

I titolari del trattamento sono tenuti al ricevimento delle segnalazioni individuando preventivamente, e sotto la logica dei principi privacy e security by design, idonee misure tecniche e organizzative volte ad evitare che si verifichino rischi per i diritti e le libertà degli interessati. Nel processo sarà quindi importante mappare il flusso dei dati, adottando misure di sicurezza specifiche, sia da un punto di vista tecnologico che fisico. La finalità dovrà essere quella di predisporre un canale di segnalazione in grado di rispettare tanto la riservatezza del segnalante, quanto l'esattezza del processo instaurato. Invero, l'art. 6 comma 1 lett. b) sancisce il diritto per il segnalante di adire l'Autorità competente, l'ANAC, qualora la segnalazione interna effettuata non abbia avuto seguito. In tal caso, l'Autorità potrebbe dar seguito ad un'indagine circa la corretta gestione della segnalazione. A tal uopo, si segnala che l'art. 21 prevede uno specifico piano sanzionatorio con un massimo edittale di cinquanta mila euro nell'ipotesi in cui venga accertato che non siano stati istituiti canali idonei di segnalazione o qualora la segnalazione sia stata ostacolata o sia stata violata la riservatezza dei soggetti.

Infine, il comma 6 dell'art. 13 del D.Lgs. n. 24/2023 prevede che i soggetti destinatari della normativa debbano adottare le misure idonee a proteggere i dati personali dei segnalanti sulla base dello svolgimento di una valutazione d'impatto ai sensi dell'art. 35 del GDPR.

In aggiunta a quanto già succitato circa l'importanza del processo di Data Governance, il comma 6 dell'art. 13 in esame richiede di prendere in considerazione nella valutazione d'impatto i rischi inerenti ai fornitori che partecipano al processo di segnalazione. A tal uopo si ricorda, che applicazione dell'art. 28 del GDPR implica una preventiva analisi circa le garanzie offerte dai responsabili del trattamento. Come ribadito, a più battute, dall'Autorità Garante ricade sul Titolare del trattamento l'onere di verificare l'adozione di misure specifiche da parte del responsabile del trattamento prima di affidare l'incarico.

Per quanto riguarda il periodo di **Data Retention** l'art. 14 del D.Lgs. n. 24/2023 prevede che le segnalazioni, interne ed esterne, nonché la relativa documentazione, **deve essere conservata nel rispetto del principio di limitazione della conservazione, e in ogni caso, per un periodo non superiore a 5 anni che decorre dalla data dell'esito finale della procedura di segnalazione.**

Ulteriormente, si ricorda la necessità di aggiornare il registro delle attività di trattamento di cui all'art. 30 del GDPR.

2.12. DIVIETO DI RITORSIONE – COSA SI INTENDE PER RITORSIONE

Qualsiasi **comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile, o della divulgazione pubblica e che provoca o può provocare, alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto, da intendersi come danno ingiustificato.**

Esempi di comportamenti ritorsivi:

- il licenziamento, la sospensione o misure equivalenti;
- la retrocessione di grado o la mancata promozione;
- il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
- la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
- le note di merito negative o le referenze negative;
- l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
- la coercizione, l'intimidazione, le molestie o l'ostracismo;
- la discriminazione o comunque il trattamento sfavorevole;
- la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
- il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
- i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
- l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
- la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
- l'annullamento di una licenza o di un permesso;
- la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

La gestione delle comunicazioni di ritorsioni nel settore privato compete ad Anac che può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato della funzione pubblica e dell'Ispettorato nazionale del lavoro.

ANAC deve accertare che il comportamento (atto o omissione) ritenuto ritorsivo sia conseguente alla segnalazione, denuncia o divulgazione.

Una volta che il segnalante provi di aver effettuato una segnalazione in conformità alla normativa e di aver subito un comportamento ritenuto ritorsivo, spetta al datore di lavoro l'onere di provare che tale comportamento non è in alcun modo collegato alla segnalazione.

Trattandosi di una presunzione di responsabilità, è necessario che le prove in senso contrario emergano nel contraddittorio davanti ad ANAC. A tal fine è fondamentale che il presunto responsabile fornisca tutti gli elementi da cui dedurre l'assenza della natura ritorsiva della misura adottata nei confronti del segnalante.

La protezione si applica anche:

- al facilitatore (persona fisica che assiste il segnalante nel processo di segnalazione e operante all'interno del medesimo contesto lavorativo);
- alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;
- ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;
- agli enti di proprietà della persona segnalante o per i quali le stesse persone lavorano nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone.

Non è punibile chi riveli o diffonda informazioni sulle violazioni:

- coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o
- relative alla tutela del diritto d'autore o
- alla protezione dei dati personali ovvero
- se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.

2.13. LE TUTELE E LE PERDITE DELLE TUTELE

Un asse portante dell'intera disciplina è rappresentato dal sistema di tutele offerte a colui che segnala, effettua una divulgazione pubblica o denuncia violazioni, tutele che si estendono anche a soggetti diversi dal segnalante e denunciante che, proprio in ragione del ruolo assunto nell'ambito del processo di segnalazione e/o del particolare rapporto che li lega al segnalante, potrebbero essere destinatari di ritorsioni.

Il d.lgs. n. 24/2023 ha previsto un sistema di protezione che comprende:

- La tutela della riservatezza del segnalante, del facilitatore, della persona coinvolta e delle persone menzionate nella segnalazione.

- La tutela da eventuali ritorsioni adottate dall'ente in ragione della segnalazione, divulgazione pubblica o denuncia effettuata e le condizioni per la sua applicazione.
- Le limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni che operano al ricorrere di determinate condizioni.

Inoltre, al fine di rafforzare l'efficacia delle tutele previste dal decreto, il legislatore ha previsto misure di sostegno al segnalante da parte di enti del Terzo settore inseriti in un apposito elenco pubblicato da ANAC.

Il nuovo decreto vieta poi, in generale, rinunce e transazioni - non sottoscritte in sede protetta 21 - dei diritti e dei mezzi di tutela ivi previsti. Si tratta degli accordi conclusi in sede giudiziale (art. 185 c.p.c); dinanzi alla commissione di conciliazione istituita presso la direzione territoriale del lavoro (art.410 c.p.c); innanzi alle sedi di certificazione (art. 31, co. 13, L. 183/2010); innanzi alla commissione di conciliazione istituita in sede sindacale (art. 412-ter c.p.c.); presso i collegi di conciliazione ed arbitrato irrituale (art. 412-quater c.p.c.). Tale previsione risponde all'esigenza di implementare e rendere effettiva la protezione del whistleblower, quale soggetto vulnerabile, nonché degli altri soggetti tutelati, che, per effetto della segnalazione, divulgazione o denuncia, potrebbero subire effetti pregiudizievoli.

L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate **senza il consenso espresso della stessa persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.**

Come è garantita la riservatezza del segnalante nell'ambito giurisdizionale?

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

Come è garantita la riservatezza del segnalante nell'ambito del procedimento disciplinare?

- Nell'ambito del procedimento disciplinare, l'identità della persona 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. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità.

I corollari della tutela della identità del segnalante:

- a) preferenza per la gestione informatizzata delle segnalazioni, con il ricorso a strumenti di crittografia;

b) sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della l., n. 241/1990 e accesso civico generalizzato ex art. 5 del d.lgs. n. 33/2013;

c) rispetto dei principi in materia di protezione dei dati personali.

La riservatezza, oltre che all'identità del segnalante, viene garantita anche a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante.

La riservatezza viene garantita anche nel caso di segnalazioni - interne o esterne - effettuate in forma orale attraverso linee telefoniche o, in alternativa, sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto con chi tratta la segnalazione

Si tutela la riservatezza del segnalante anche quando la segnalazione perviene a personale diverso da quello autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo

In due casi espressamente previsti dal decreto, per rivelare l'identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione:

- nel procedimento disciplinare laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare;
- nei procedimenti instaurati in seguito a segnalazioni interne o esterne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

Le tutele non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave; in tali casi alla persona segnalante o denunciante può essere irrogata una sanzione disciplinare.

2.14. MISURE DI SOSTEGNO AI SEGNALANTI

Sono previste misure di sostegno che consistono in informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni offerta dalle disposizioni normative nazionali e da quelle dell'Unione europea, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato.

È istituito presso l'ANAC l'elenco degli enti del Terzo settore che forniscono alle persone segnalanti misure di sostegno.

2.15. SANZIONI PER LE VIOLAZIONI APPLICATE DA ANAC

Sanzioni **applicabili da Anac**:

- da 10.000 a 50.000 euro quando accerta che sono state commesse ritorsioni o quando accerta che la segnalazione è stata ostacolata o che si è tentato di ostacolarla o che è stato violato l'obbligo di riservatezza;
- da 10.000 a 50.000 euro quando accerta che non sono stati istituiti canali di segnalazione, che non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme a quella richiesta dalla legge, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute;
- da 500 a 2.500 euro, nel caso di perdita delle tutele, salvo che la persona segnalante sia stata condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile.

3. ADEMPIMENTI WHISLTEBLOWING DA PARTE DI CENTROFOR

Conclusa la valutazione preliminare si passa ora alla descrizione delle attività da svolgersi da parte dei soggetti coinvolti nella gestione del canale.

3.1. COMPITI DEL PRESIDENTE DEL CDA

Il Presidente del Cda di CENTROFOR deve:

1. Far approvare dal Cda le modifiche adottate del Modello organizzativo nella parte generale introducendo sanzioni per:
 - a) la commissione di atti ritorsivi nei confronti del segnalante (con riferimento e quanto previsto dall'art 17 d. lgs 24/2023);
 - b) La mancata istituzione di canali di segnalazione;
 - c) La mancata adozione di procedure per l'effettuazione e la gestione delle segnalazioni;
 - d) adozione di procedure non conformi a quelle previste;
 - e) condotte di ostacolo alla segnalazione;
 - f) violazioni dell'obbligo di riservatezza della segnalazione;
 - g) omessa attività di verifica e analisi delle segnalazioni ricevute.
2. Predisporre e/o successivamente revisionare la procedura Whistleblowing e farla adottare dal C.d.A., unitamente al Modello modificato, sentite le rappresentanze o le organizzazioni sindacali (ai sensi dell'art. 51, D.Lgs. n. 81/2015, si tratta delle organizzazioni sindacali comparativamente più rappresentative sul piano nazionale, delle rappresentanze sindacali aziendali di queste ultime ovvero dalla rappresentanza sindacale unitaria);
3. nominare con atto scritto gli incaricati del trattamento;

4. attribuire con atto scritto la nomina di responsabile del trattamento sotto il profilo privacy al gestore del canale, eventualmente nominando per iscritto eventuali incaricati (soggetto Responsabile ed eventuali incaricati);
5. attribuire con atto scritto la nomina di responsabile del trattamento sotto il profilo privacy al soggetto che gestisce sotto il profilo informatico il canale informatico da utilizzare per le segnalazioni, eventualmente nominando per iscritto eventuali incaricati (soggetto Responsabile ed eventuali incaricati);
6. prevedere due o più canali di segnalazione per ogni categoria di segnalazioni, secondo le indicazioni previste più oltre al paragrafo 5.2;
7. fornire istruzioni ai soggetti incaricati della gestione del canale di segnalazione;
8. Prevedere l'obbligo di restituzione di informazioni al gestore del canale in caso di raccomandazione o di richiesta di modifiche all'esito della gestione delle eventuali segnalazioni;
9. Inviare comunicazione al gestore di eventuali provvedimenti disciplinari o di iniziative giudiziarie intraprese in caso di segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa segnalazione.

3.1.1. ADEMPIMENTI PER GARANTIRE LA PROTEZIONE DEI DATI PERSONALI

Di seguito vengono sintetizzati i principali adempimenti che occorre rispettare in ottica Data Protection alla luce del framework di riferimento, incluso anche il Decreto.

IL TITOLARE DEL TRATTAMENTO PRIVACY DEVE

1. Provvedere ad una valutazione di impatto (Data Protection Impact Assessment – DPIA); considerata la particolare delicatezza delle informazioni trattate, della vulnerabilità degli interessati, nonché degli elevati rischi –in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante– il trattamento svolto nell'ambito del whistleblowing deve considerarsi ad alto rischio ed è quindi obbligatorio lo svolgimento di una valutazione d'impatto, preventiva al trattamento;
2. trattare i dati secondo quanto previsto dall'art. 13 d. lgs.24/2023, tenendo conto di quanto già trattato al precedente punto 2.12;
3. Rendere ex ante ai possibili interessati un'informativa sul trattamento dei dati personali mediante la pubblicazione di documenti informativi (ad esempio sul sito web, oppure informative brevi in occasione dell'uso di altre modalità scritte o orali)
4. Assicurare l'aggiornamento del registro delle attività di trattamento
5. Garantire il divieto di tracciamento dei canali di segnalazione

6. Garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante
7. mettere in atto tutte le misure affinché nel trattamento dei dati vengano rispettati i principi previsti dalla legge, tra cui quelli di liceità, correttezza, trasparenza, limitazione della finalità, esattezza, limitazione della conservazione, integrità, riservatezza e responsabilizzazione e fornire specifiche e dettagliate istruzioni agli altri soggetti rilevanti ai fini privacy (Responsabile, incaricati);
8. mettere in atto misure adeguate di *privacy by design e by default*:
 - a) MINIMIZZAZIONE: i dati personali che non sono utili al trattamento di una specifica segnalazione non devono essere raccolti. Se vengono raccolti accidentalmente, devono essere cancellati (art. 13 d. lgs cit.);
 - b) TRASPARENZA RAFFORZATA: in materia di whistleblowing occorre porre particolare attenzione alla completezza delle informazioni in relazione a ciascun trattamento, fornendo informative chiare e complete agli interessati. Dovrà essere predisposta una **adeguata informativa da pubblicare sul sito**;
 - c) AUTORIZZAZIONI AL TRATTAMENTO: è necessario che **i soggetti preposti alla gestione delle segnalazioni ricevano adeguate nomine, redatte per iscritto**, includendo fra gli obblighi cui è tenuto l'autorizzato al trattamento anche la riservatezza (con le precisazioni contenute nell'art. 12 del d. lgs 24/2023);
 - d) REGISTRO DEI TRATTAMENTI: dovrà essere istituito e compilato il registro dei trattamenti; istruzioni in tale senso dovranno essere date ai responsabili e agli incaricati. Occorre indicare nel registro dei trattamenti la finalità di acquisizione e gestione di segnalazioni di condotte illecite e tutte le ulteriori informazioni richieste dalla legge;
 - e) PROCEDURE: l'adozione di procedure o policy inerenti alla gestione delle segnalazioni e la protezione dei dati personali nei trattamenti è fondamentale per la legittimità dei trattamenti in questione, nel rispetto del principio di accountability, anche ai sensi degli artt. 5 e 24 del GDPR.
 - f) MISURE DI SICUREZZA: è necessario adottare tutte quelle misure adeguate per assicurare, su base permanente, la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento.

Il titolare dovrà provvedere altresì:

1. ALLA GESTIONE DEI DIRITTI DEGLI INTERESSATI: il titolare del trattamento deve adottare le necessarie misure (tra cui, ad esempio, la predisposizione di una procedura ad hoc o la formazione del personale a ciò preposto) affinché, in caso di esercizio dei diritti privacy, venga dato tempestivamente l'adeguato riscontro. Le procedure adottate dovranno tenere conto anche dei limiti previsti dalla legge (in particolare dall'art. 2 *undecies* del Codice Privacy, nonché di quanto

stabilito dall'art 12 comma 2 e 8 d. lgs 24/2024): i diritti previsti dal GDPR non possono infatti essere esercitati qualora possa derivarne un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante.

3. A VALUTARE PREVIAMENTE L'IDONEITÀ DEL RESPONSABILE: - anche con riferimento alle misure di sicurezza che offre, agli eventuali subresponsabili che coinvolge e alla possibile conservazione dei dati fuori dall'UE - e poi formalizzare un contratto ai sensi dell'art. 28 del GDPR sufficientemente tutelante.
4. AD EFFETTUARE AUDIT: per verificare che gli obblighi assunti contrattualmente dal fornitore risultino applicati;
5. A PROVVEDERE ALLA CONSERVAZIONE DEI DATI: secondo i criteri indicati nel precedente paragrafo 2.12.
6. FORMAZIONE: come in ogni contesto di trattamento di dati personali, ma a maggior ragione in un ambito delicato come quello del Whistleblowing, è necessario che il titolare si occupi della formazione delle persone che agiscono sotto la propria autorità.

4. I COMPITI DEL GESTORE DELLA SEGNALAZIONE

Il canale interno è gestito dall'O.d.V. 231 di CENTROFOR che è incaricato e riveste quindi il ruolo di gestore del canale interno ai sensi e per gli effetti di cui all'art. 4 D.L.vo 24/2023; **l'incarico deve essere redatto per iscritto.**

L'Organismo di Vigilanza si occupa di gestire:

- I. tutti gli illeciti amministrativi, contabili, civili o penali (diversi da quelli richiamati nelle singole disposizioni normative dell'Allegato);
- II. le condotte illecite «rilevanti» ai sensi del D.L.vo. 231/2001. Da intendersi quale richiamo alle singole fattispecie di reato in esso espressamente menzionate (elencazione tassativa); e/o delle violazioni dei modelli, vale a dire violazioni che riguardano le regole scritte nel Modello - tipicamente nella Parte Speciale dello stesso o nel Codice Etico;
- III. gli illeciti relativi ai n. 3), 4), 5) e 6), lett. a) dell'art. 2 D.L.vo 24/ 2023, riguarda gli illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'Allegato al Decreto; atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'art. 325, Trattato sul funzionamento dell'Unione europea; o atti od omissioni riguardanti il mercato interno di cui all'art. 26, par. 2, Trattato.

L'O.d.V. nella gestione della segnalazione rispetta i rispetta le norme previste dagli articoli:

Art. 5 - Gestione del canale di segnalazione interna;

Art. 12 - Obbligo di riservatezza;

Art. 13 - Trattamento dei dati personali;

Art. 14 - Conservazione della documentazione inerente alle segnalazioni;

Art. 16 - Condizioni per la protezione della persona segnalante;

Art. 17 - Divieto di ritorsione;

Art. 19 - Protezione dalle ritorsioni.

Per una valutazione ragionata delle modalità e dei relativi controlli e delle protezioni si vedano sopra i paragrafi da 2 a 2.16.

Il **gestore della segnalazione** deve:

1. partecipare alla formazione specifica che CENTROFOR riterrà di disporre;
2. provvedere alla propria formazione sulla normativa whistleblowing;
3. provvedere alla formazione dei possibili segnalanti, predisponendo eventualmente schede informative
4. Definire il proprio modello di ricevimento e gestione delle segnalazioni interne ai sensi dell'art 13 del d. lgs.24/2023, provvedendo:
 - a) a filtrare i casi rilevanti (valutando la pertinenza del messaggio ricevuto: la segnalazione viola un diritto dell'Unione Europa così come tutelato dalla Direttiva UE sul Whistleblowing? Oppure una normativa nazionale? Oppure ancora le vostre policy interne, il Modello e il codice etico? In caso contrario, è necessario informare il segnalante circa l'inappropriatezza della segnalazione e comunicare quale sarebbe stato il canale alternativo dove denunciare il fatto), provvedendo se del caso alla immediata archiviazione in caso di accertamento della infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti (il riscontro può ad esempio consistere nella comunicazione dell'archiviazione della procedura per mancanza di prove sufficienti o altri motivi, o perché riguardante una delle ipotesi previste dall'art. 1, co. 1, lett. a), b) e c) del D.L.vo 24/2023 (riportate al precedente punto 2.1). o per il caso di accertato contenuto generico della segnalazione di illecito tale da non consentire la comprensione dei fatti ovvero segnalazione di illeciti corredata da documentazione non appropriata o inconferente.
 - b) stabilire una comunicazione con il segnalante il più presto possibile **e comunque entro 7 giorni dal momento della ricezione della segnalazione**; se il segnalante ha inviato un recapito contestualmente il gestore provvede ad inviare al segnalante una informativa whistleblowing secondo lo schema predisposto e concordato con Cda e titolare del trattamento privacy;
 - c) dare **riscontro entro 3 mesi decorrenti dal momento dell'invio dell'avviso di ricezione della segnalazione**; il riscontro può consistere nella comunicazione dell'archiviazione, nell'avvio di un'inchiesta interna ed eventualmente nelle relative risultanze, nei provvedimenti adottati per affrontare la questione sollevata, nel rinvio a un'autorità competente per ulteriori indagini. Il medesimo riscontro, da rendersi nel termine di tre mesi, può anche essere

meramente interlocutorio, giacché possono essere comunicate le informazioni relative a tutte le attività sopra descritte che si intende intraprendere e lo stato di avanzamento dell'istruttoria; in tale ultimo caso, terminata l'istruttoria, gli esiti dovranno comunque essere comunicati alla persona segnalante;

- d) Avviare se del caso e comunque nei tempi stabiliti dalla normativa l'istruttoria del caso eventualmente inviando comunicazioni interlocutorie al segnalante
- e) istituire registro delle segnalazioni avente data certa quanto all'inserimento delle singole segnalazioni;
- f) chiudere la segnalazione con l'archiviazione e/o l'indicazione dei provvedimenti adottati;
- g) inviare anche per estratto la motivazione dei provvedimenti adottati al segnalante;
- h) dopo il completamento di qualsiasi indagine, riassumere i risultati per il management, comprese le eventuali misure correttive che sono raccomandate al fine dell'eventuale adozione;
- i) inviare se del caso una specifica raccomandazione al Cda in relazione alla quale:
 - I. alla conclusione dell'approfondimento svolto, sottoporre i risultati alla valutazione al Cda a seconda dell'oggetto della segnalazione, affinché vengano intrapresi i più opportuni provvedimenti;
 - II. concordare con il management responsabile della funzione interessata dalla segnalazione, l'eventuale "action plan" necessario per la rimozione delle debolezze di controllo rilevate;
 - III. dare informazione al Cda delle segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa segnalazione;
 - IV. acquisire l'avvio di un procedimento disciplinare nei confronti del segnalante, nel caso di segnalazioni in relazione alle quali siano accertate la malafede del segnalante e/o l'intento meramente diffamatorio, eventualmente confermati anche dalla infondatezza della stessa segnalazione;

Le attività sopra descritte non sono necessariamente svolte in maniera sequenziale.

5. ISTITUZIONE DEL CANALE DI SEGNALAZIONE E MODALITA' DELLA SEGNALAZIONE

5.1. CANALE DI SEGNALAZIONE – IN GENERALE

La segnalazione può essere inviata in qualsiasi forma tra quelle indicate nell'art. 4 comma 3 D.L.vo 24/2023, secondo le modalità più oltre descritte; per le dichiarazioni inviate per iscritto è disponibile un **fac-simile di "Modulo segnalazione"**, **allegato alla presente procedura**.

Il segnalante dovrà riportare nella segnalazione scritta le seguenti informazioni:

- a) descrizione della condotta illecita;

- b) identità del soggetto che effettua la segnalazione, con indicazione di qualifica/funzione/ruolo svolto;
- c) chiara e completa descrizione dei fatti oggetto di segnalazione;
- d) qualora conosciute, le circostanze di tempo e di luogo in cui i fatti sono stati commessi;
- e) qualora conosciute, le generalità o altri elementi che consentano di identificare il soggetto che ha posto in essere i fatti segnalati;
- f) eventuali ulteriori soggetti che possono riferire sui fatti oggetto di segnalazione;
- g) eventuali ulteriori documenti che possono confermare la fondatezza di tali fatti;
- h) ogni ulteriore informazione che possa fornire un utile riscontro circa la sussistenza dei fatti segnalati.

5.2 CANALI DI SEGNALAZIONI PREDISPOSTI DA CENTROFOR

CENTROFOR ha incaricato per la gestione delle segnalazioni il proprio Organismo di Vigilanza.

Tutte le comunicazioni da parte del segnalante nei confronti dell'Organismo di Vigilanza possono essere effettuate, alternativamente e senza preferenza:

1) PER ISCRITTO A MEZZO DI:

Nota/lettera a mezzo del servizio postale in busta chiusa recante la dicitura "RISERVATA NON APRIRE – DA CONSEGNARE ALL'ORGANISMO DI VIGILANZA – GESTORE CANALE WHISTLEBLOWING". Secondo quanto previsto dalla delibera ANAC 311 DEL 12 luglio 2023; a tale fine ed in vista della protocollazione riservata della segnalazione a cura del gestore, è necessario che la **segnalazione venga inserita in due buste chiuse**: la prima con i dati identificativi del segnalante unitamente alla fotocopia del documento di riconoscimento; la seconda con la segnalazione, in modo da separare i dati identificativi del segnalante dalla segnalazione. Entrambe dovranno poi essere inserite in una terza busta chiusa che rechi all'esterno la dicitura sopra richiamata⁵. La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

L'indirizzo di posta ordinaria è:

Organismo di Vigilanza c/o CENTROFOR Via Ragazzi del 99, n. 35 - TRENTO

2) CANALE DI POSTA ELETTRONICA

La segnalazione della violazione può essere inoltrata tramite e-mail, apposita casella di posta elettronica dedicata firmata o in forma anonima al seguente indirizzo odv.centrofor@gmail.com

Il canale di posta elettronica è visibile solo ad ODV gestore delle segnalazioni e gestita tramite password conosciuta esclusivamente da ODV e modificata trimestralmente.

⁵ La forma della segnalazione cartacea è ripresa dalle Linee Guida Anac del 12.07.2023

3) FORMA ORALE

La forma orale è consentita previa richiesta da parte del Segnalante di un incontro diretto (attraverso mail o con la modalità scritta sopra riportata o **telefonando al numero 0461.239136 dello Studio Dike Avvocati Associati**) con l'Organismo di Vigilanza, **che fisserà l'incontro entro un termine ragionevole. L'incontro, allaverrà registrato.**

CENTROFOR garantendo la riservatezza sull'identità del segnalante, incoraggia i destinatari a non effettuare segnalazioni anonime, in modo da consentire al gestore della segnalazione di eventualmente chiedere approfondimenti e integrazioni indispensabili per garantire diligente seguito alla segnalazione stessa.

È inoltre **consigliato indicare chiaramente nell'oggetto della segnalazione che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele approntate dal D.Lgs. 24/2023.**

Tale specificazione consente, laddove la segnalazione pervenga erroneamente ad un soggetto non competente oppure attraverso un canale diverso da quelli specificamente previsti dal decreto e adottati da CENTROFOR, la trasmissione tempestiva da parte di quest'ultimo al soggetto autorizzato a ricevere e gestire le segnalazioni di whistleblowing.

5.3. CANALE ESTERNO E DIVULGAZIONE PUBBLICA

Si veda sopra il paragrafo.

6. ARCHIVIAZIONE DELLA DOCUMENTAZIONE

L'O.d.V. è tenuto a documentare, mediante la conservazione di documenti informatici e/o cartacei, le segnalazioni ricevute, al fine di garantire la completa tracciabilità degli interventi intrapresi per l'adempimento delle sue funzioni istituzionali.

I documenti in formato elettronico sono conservati in una "directory" protetta con accesso solo per i soggetti espressamente autorizzati dall'O.d.V., protetto da doppia password (a protezione del programma di gestione e a protezione del relativo fascicolo)

L'archivio cartaceo è conservato in armadio chiuso a chiave presso lo Studio DIKE AVVOCATI ASSOCIATI.

L'archivio informatico è protetto con doppia password dedicata modificata trimestralmente.

In caso di segnalazioni prodotte in evidente malafede in coerenza con quanto enunciato ai punti 6.1 (anonimato) e 7 (Modalità di segnalazione) della presente procedura, l'O.d.V. si riserva di archiviare le stesse cancellando i nomi e gli elementi che possano consentire l'identificazione dei soggetti segnalati.

7. LIMITI DELLA TUTELA – RESPONSABILITA' DEL SEGNALANTE

La tutela prevista dalla norma è circoscritta all'ambito interno, operando sostanzialmente in ambito disciplinare ed all'interno del rapporto di lavoro.

Quanto alla non punibilità dei segnalanti si rileva che non è punibile chi riveli o diffonda informazioni sulle violazioni:

- coperte dall'obbligo di segreto, diverso da quello professionale forense e medico, o
- relative alla tutela del diritto d'autore o
- alla protezione dei dati personali ovvero se, al momento della segnalazione, denuncia o divulgazione, aveva ragionevoli motivi di ritenere che la rivelazione o diffusione delle informazioni fosse necessaria per effettuare la segnalazione e la stessa è stata effettuata nelle modalità richieste dalla legge.

Quanto alla perdita delle tutele: le tutele non sono garantite quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona segnalante per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'autorità giudiziaria o contabile ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave; in tali casi alla persona segnalante o denunciante può essere irrogata una sanzione disciplinare.

Qualora a seguito degli accertamenti interni effettuati dall'O.d.V., la segnalazione risulti manifestamente infondata ed effettuata per finalità opportunistiche o al solo scopo di danneggiare il denunciato o altri soggetti, l'O.d.V. segnala l'esito degli accertamenti al C.d.A. per i provvedimenti di competenza anche con riguardo alla responsabilità disciplinare a carico del segnalante.

8. DISPOSIZIONI FINALI

La presente procedura sarà sottoposta a revisione periodica per verificare possibili lacune o incomprensioni da parte dei dipendenti.

Per quanto non previsto nel presente documento si rinvia alle fonti normative richiamate in premessa.

9. PUBBLICITA'

La presente procedura, unitamente al Modulo per la segnalazione di condotte illecite è pubblicata nel sito web: www.centrofor.com.