CITTÀ METROPOLITANA DI GENOVA

Atto dirigenziale

Segreteria e Direzione Generale

Atto N. 2469/2023

Oggetto: DISCIPLINA DELLA PROCEDURA E DELLLE MODALITA' DI PRESENTAZIONE E GESTIONE DELLE SEGNALAZIONI DI ILLECITI IN CITTA' METROPOLITANA DI GENOVA (WHISTLEBLOWING).

In data 31/10/2023 il dirigente MARIA CONCETTA GIARDINA, nella sua qualità di responsabile, adotta il seguente Atto dirigenziale;

Vista la Legge 7 aprile 2014 n. 56, “Disposizioni sulle città metropolitane, sulle province, sulle unioni e fusioni di comuni”;

Richiamato il vigente Statuto della Città Metropolitana di Genova;

VISTI

- l’art. 107, commi 1, 2 e 3, del Decreto Legislativo 18 agosto 2000, n. 267, “Testo unico delle leggi sull’ordinamento degli enti locali”.
- la legge 6 novembre 2012, n. 190 «Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione»;
- la 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;
- il Decreto legislativo 10 marzo 2023, n. 24 recante 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. (Decreto whistleblowing);
- le Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne, approvate con Delibera n°311 del 12 luglio 2023

RICHIAMATI

- il Decreto legislativo 30 giugno 2003, n. 196 (Codice in materia di protezione dei dati personali), nel testo vigente a seguito dell’entrata in vigore del Decreto Legislativo 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
- il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (RGPD);

CITTÀ METROPOLITANA DI GENOVA

Atto dirigenziale

Segreteria e Direzione Generale

CONSIDERATO

- che con Decreto del Sindaco Metropolitano n. 7 del 27/01/2023 Il Segretario Generale e Direttore Generale Dott.ssa Giardina Maria Concetta è individuata quale Responsabile della prevenzione della corruzione e per la trasparenza – RPCT
- che il Responsabile della Prevenzione della Corruzione e della Trasparenza rende noto il numero delle segnalazioni ricevute e il loro stato di avanzamento all'interno della relazione annuale di cui all'art. 1, comma 14, della Legge n. 190/2012, garantendo l'anonimato;

RITENUTO NECESSARIO disciplinare, con atto organizzativo specifico, le disposizioni interne in materia, a superamento di quanto già previsto con Direttiva del Responsabile Prevenzione Corruzione e Trasparenza (RPCT) Prot. n. 55159 /20 “Gestione delle segnalazioni di condotte illecite (cd. Whistleblowing) di Città Metropolitana di Genova “ del 28 Dicembre 2020 alla luce delle nuove modifiche normative;

ACQUISITO il parere del Responsabile della Protezione dei dati personali (RPD);

SENTITE le Organizzazioni sindacali di cui all’art. 51 D. Lgs. 81/2015

VISTO il Decreto del Sindaco metropolitano n. 9 del 30 gennaio 2023 con cui sono stati approvati il Piano Integrato di Attività e Organizzazione (PIAO) e il Piano Esecutivo di Gestione finanziario (PEG) per il triennio 2023-2025;

Dato atto che l’istruttoria del presente atto è stata svolta da GIULIA LEVRERO, responsabile del procedimento, che attesta la regolarità e correttezza dell’azione amministrativa per quanto di competenza, ai sensi dell’articolo 147 bis del decreto legislativo n. 267/2000 e che provvederà a tutti gli atti necessari all’esecuzione del presente provvedimento, fatta salva l’esecuzione di ulteriori adempimenti posti a carico di altri soggetti;

Considerato che con la sottoscrizione del presente atto, il dirigente attesta altresì la regolarità e correttezza dell’azione amministrativa, assieme al responsabile di procedimento ai sensi dell’articolo 147 bis del decreto legislativo n. 267/2000;

Dato atto che il presente provvedimento non ha implicazioni contabili o finanziarie;

DISPONE

1) di adottare, a superamento del Direttiva del Responsabile Prevenzione Corruzione e Trasparenza (RPCT) Prot. n. 55159 /20 “*Gestione delle segnalazioni di condotte illecite (cd. Whistleblowing) di Città Metropolitana di Genova*“ del 28 Dicembre 2020, il seguente atto organizzativo interno che, in conformità al D. Lgs. 24/2023, disciplina le modalità e le procedure adottate dalla Città Metropolitana di Genova a garanzia della protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell’Unione europea che ledano l’interesse pubblico o l’integrità dell’amministrazione pubblica di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato nonché tenuto conto delle Linee guida e i suoi approfondimenti in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e violazioni delle disposizioni normative nazionali;
2) di dare atto che tali modalità e procedure sono ad ogni effetto integrative di quelle già

CITTÀ METROPOLITANA DI GENOVA

Atto dirigenziale

Segreteria e Direzione Generale

assegnate dal Titolare del trattamento ai sensi del combinato disposto di cui agli articoli 29 del RGPD e 2-quaterdecies del Codice in materia di protezione dei dati personali, ferme le responsabilità disciplinari previste per violazione degli appositi doveri di comportamento, nonché per mancato rispetto delle norme sulla protezione dei dati personali richiamate dal codice di comportamento in vigore;

3) di autorizzare, come previsto dall'art. 12 del d.lgs. 24/2023, le persone competenti a ricevere o a dare seguito alle segnalazioni al trattamento dei dati relativi all'identità del segnalante nonché al trattamento di ogni altro dato o informazione personale contenuta nelle segnalazioni medesime;
4) di pubblicare il presente provvedimento nella sezione Amministrazione Trasparente del sito istituzionale, su apposita pagina web del sito istituzionale e nella intranet di Città Metropolitana di Genova;
5) di richiamare il contenuto del presente provvedimento all'interno del Piano Integrato di Attività ed Organizzazione (P.I.A.O)
6) di pianificare iniziative di sensibilizzazione e formazione del personale per divulgare le finalità dell'istituto del whistleblowing e la procedura per il suo utilizzo

Sottoscritta dal Dirigente
(MARIA CONCETTA GIARDINA)
con firma digitale

WHISTLEBLOWING

Disciplina adottata da Città Metropolitana di Genova

Sommario

1 Premessa[1]

Il decreto legislativo 10 marzo 2023, n. 24 recepisce in Italia la 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.

La nuova disciplina è orientata, da un lato, a garantire la manifestazione della libertà di espressione e di informazione; dall'altro, è strumento per contrastare (e prevenire) la corruzione, la *maladministration* e la prevenzione di violazioni di legge nel settore pubblico e privato.

Il segnalante si pone nelle condizioni di fornire informazioni tali da condurre all'indagine, all'accertamento e al perseguimento di fenomeni corruttivi o comunque di fatti illeciti. In tal modo il soggetto fornisce il proprio contributo all'azione responsabile da parte delle istituzioni democratiche.

La norma nazionale garantisce la protezione, nelle differenti articolazioni di tutela della riservatezza e di copertura da fenomeni di ritorsione, dei soggetti che si espongano con segnalazioni, denunce o con il nuovo istituto della divulgazione pubblica. Tale protezione viene peraltro oggi estesa a soggetti diversi da chi segnala, quali il facilitatore o comunque le persone menzionate nella segnalazione: i legislatori europeo e nazionale hanno infatti inteso rafforzare l'istituto in questione, potenziandone la funzione di presidio per la legalità, nonché per il buon andamento e l'imparzialità delle pubbliche amministrazioni.

L'Autorità Nazionale Anticorruzione (di seguito ANAC) ha predisposto, nel giugno 2023, uno schema di Linee Guida, qui in larga parte richiamate nella descrizione testuale dell'istituto, posto in consultazione a tutto il 15 giugno 2023 poi approvate con Delibera n°311 del 12 luglio 2023.

Tali Linee Guida, pur volte a dare solo indicazioni per la presentazione e gestione delle segnalazioni esterne in capo all'Autorità ai sensi dell'art. 10 del D. Lgs. 24/2023, sono state proposte anche al fine di fornire indicazioni e principi di cui gli enti pubblici e privati possono tenere conto per i propri canali e modelli organizzativi interni.

Le principali novità contenute nella nuova disciplina vengono richiamate da ANAC come di seguito:

- ✓ specificazione dell'ambito soggettivo con riferimento agli enti di diritto pubblico, di quelli di diritto privato e estensione del novero di questi ultimi;
- ✓ ampliamento del novero dei soggetti, persone fisiche, che possono essere protetti per le segnalazioni, denunce o divulgazioni pubbliche;
- ✓ espansione dell'ambito oggettivo, cioè di ciò che è considerato violazione rilevante ai fini della protezione nonché distinzione tra ciò che è oggetto di protezione e ciò che non lo è;
- ✓ disciplina di tre canali di segnalazione e delle condizioni per accedervi: interno (negli enti con persona o ufficio dedicato oppure tramite un soggetto esterno con competenze specifiche), esterno (gestito da ANAC) nonché il canale della divulgazione pubblica (tramite stampa o social media);
- ✓ indicazione di diverse modalità di presentazione delle segnalazioni, in forma scritta o orale;
- ✓ disciplina dettagliata degli obblighi di riservatezza e del trattamento dei dati personali ricevuti, gestiti e comunicati da terzi o a terzi;
- ✓ chiarimenti su che cosa si intenda per ritorsione e ampliamento della relativa casistica;
- ✓ specifiche sulla protezione delle persone segnalanti o che comunicano misure ritorsive offerta sia da ANAC che dall'autorità giudiziaria e maggiori indicazioni sulla responsabilità del segnalante e sulle scriminanti;
- ✓ introduzione di apposite misure di sostegno per le persone segnalanti e coinvolgimento a tal fine di

[1] Alcuni passaggi contengono riferimenti testuali alle in materia, che richiama a sua volta il D. Lgs. 24/2023

enti del Terzo settore che abbiano competenze adeguate e che prestino la loro attività a titolo gratuito;

- ✓ revisione della disciplina delle sanzioni applicabili da ANAC e introduzione da parte dei soggetti privati di sanzioni nel sistema disciplinare adottato ai sensi del d.lgs. n. 231/2001.

2 Ambito soggettivo

Il decreto legislativo n. 24/2023 individua l'ambito soggettivo di applicazione della nuova disciplina con contenuti molto innovativi rispetto alla precedente normativa. Vi sono ricompresi, tra l'altro, tutti i soggetti che si trovino **anche solo temporaneamente in rapporti lavorativi** con una amministrazione o con un ente privato, pur non avendo la qualifica di dipendenti (es. i volontari, i tirocinanti, retribuiti o meno) nonché, seppur a determinate condizioni, coloro che ancora non abbiano un rapporto giuridico con l'ente (in fase di trattative precontrattuali) ovvero coloro il cui rapporto sia cessato o che siano in periodo di prova.

La persona segnalante è quindi considerata **la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo**.

Quanto agli enti tenuti ad applicare la disciplina e tenuti a prevedere misure di tutela per il dipendente che denuncia gli illeciti, la norma si riferisce sia **soggetti del settore pubblico**, sia a **soggetti del settore privato**.

Come evidenziato da ANAC, le tipologie di soggetti pubblici o privati sono individuabili con il sistema di rinvii alle norme che, riferendosi ai soggetti da tutelare, indirettamente identificano anche i datori di lavoro di questi ultimi, dando luogo a una notevole estensione della disciplina ad enti ed imprese di diritto privato.

In parallelo, il decreto amplia notevolmente, rispetto alla precedente normativa, il novero dei soggetti a cui, all'interno del settore pubblico, viene riconosciuta protezione, anche da ritorsioni, in caso di segnalazione, interna o esterna, divulgazione pubblica e denuncia all'Autorità giudiziaria.

Per tutti i suddetti soggetti, la tutela si applica **anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico**.

Ulteriore novità del d.lgs. n. 24/2023 consiste nel fatto che la **tutela** è riconosciuta, oltre a determinati soggetti del settore pubblico e del settore privato che effettuano segnalazioni, denunce o divulgazioni pubbliche, **anche ad alcuni soggetti diversi dal segnalante** che potrebbero essere destinatari di ritorsioni anche indirette, in ragione del ruolo assunto nell'ambito del processo di segnalazione, divulgazione pubblica o denuncia e/o del particolare rapporto che li lega al segnalante o denunciante.

I soggetti tutelati diversi da chi segnala, denuncia o effettua divulgazioni pubbliche sono i seguenti:

- **Facilitatore**, persona fisica che assiste il segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;
- **Persone del medesimo contesto lavorativo** del segnalante, denunciante o di chi effettua una divulgazione pubblica **e** che sono legate ad essi da uno **stabile legame affettivo o di parentela entro il quarto grado**;
- **Colleghi di lavoro** del segnalante, denunciante o di chi effettua una divulgazione pubblica, che lavorano nel **medesimo contesto lavorativo** della stessa e che hanno con detta persona un **rapporto abituale e corrente**;
- **Enti di proprietà**, in via esclusiva o in compartecipazione maggioritaria di terzi, del segnalante, denunciante o di chi effettua una divulgazione pubblica;
- **Enti presso i quali** il segnalante, denunciante o chi effettua una divulgazione pubblica **lavorano** (art. 3, co. 5, lett. d));
- **Enti** che operano nel **medesimo contesto lavorativo** del segnalante, denunciante o di chi effettua

una divulgazione pubblica.

3 Ambito oggettivo

Oggetto di **segnalazione, denuncia e divulgazione pubblica** sono informazioni sulle **violazioni di specifiche normative nazionali e dell'Unione Europea**: il legislatore individua con una certa ampiezza le tipologie di illeciti da considerare e solo queste rilevano affinché una segnalazione, una divulgazione pubblica o una denuncia possano essere considerate ai fini dell'applicabilità della disciplina.

Nella trattazione sull'ambito oggettivo rientrano **anche** le **comunicazioni ad ANAC** delle **ritorsioni** che coloro che hanno effettuato segnalazioni, denunce o divulgazioni pubbliche ritengono di aver subito nel proprio contesto lavorativo. Anche in tal caso, la nuova disciplina si evolve rispetto alla precedente, poiché fornisce un elenco, sia pure non tassativo, di misure ritorsive, dopo aver esteso la tutela anche a soggetti diversi dal segnalante, divulgatore e denunciante.

Il nuovo d.lgs. n. 24/2023 stabilisce che sono oggetto di segnalazione, divulgazione pubblica o denuncia le informazioni sulle violazioni **che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato**.

Le informazioni possono riguardare sia le **violazioni commesse**, sia quelle **non ancora commesse** che il *whistleblower*, ragionevolmente, ritenga possano concretizzarsi. Possono essere oggetto di segnalazione, divulgazione pubblica o denuncia anche **condotte volte ad occultare le violazioni**.

Non sono ricomprese, tra le informazioni, violazioni segnalabili o denunciabili ai sensi della normativa in questione, le notizie palesemente prive di fondamento, le informazioni che sono già totalmente di dominio pubblico, nonché informazioni acquisite solo sulla base di indiscrezioni sommarie (cd. voci di corridoio).

Il legislatore ha inteso tipizzare gli illeciti, gli atti, i comportamenti o le omissioni che possono essere segnalati, divulgati o denunciati, indicando - con una tecnica di rinvio che la stessa ANAC definisce piuttosto complessa - cosa sia qualificabile come violazione.

Diversamente da quanto previsto nelle precedenti Linee Guida ANAC n. 469/2021, non sono più ricomprese, tra le violazioni segnalabili, le irregolarità nella gestione o organizzazione dell'attività.

La *ratio* di fondo è quella sempre e comunque di valorizzare i principi costituzionali di buon andamento e imparzialità dell'azione amministrativa di cui all'art. 97 Cost. nonché quello della correttezza dell'azione in capo ai soggetti che operano nell'ambito di un ente pubblico o privato, rafforzando i principi di legalità nonché della libertà di iniziativa economica e di libera concorrenza tutelati ai sensi dell'art. 41 della Cost.

Ai fini di un inquadramento completo dell'ambito oggettivo di applicazione, è indispensabile tener conto del fatto che il legislatore specifica **ciò che non può essere oggetto di segnalazione**, divulgazione pubblica o denuncia.
Si riporta di seguito la elencazione fornita da ANAC:

- Le contestazioni, rivendicazioni o richieste legate ad un **interesse di carattere personale** del segnalante o della persona che ha sporto una denuncia all'Autorità giudiziaria o contabile e che attengano 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. Sono quindi, escluse, ad esempio, le segnalazioni riguardanti vertenze di lavoro, discriminazioni tra colleghi, conflitti interpersonali tra la persona segnalante e un altro lavoratore;
- Le segnalazioni di violazioni, **laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali**, indicate nella parte II dell'allegato al decreto ovvero da disposizioni nazionali che costituiscono attuazione degli atti dell'Unione europea (indicati nella parte II dell'allegato alla

direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al decreto);

- Le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea.

  Le segnalazioni che riguardino argomenti disciplinati da **disposizioni nazionali o dell'UE** su: informazioni classificate (cd. segreto di Stato); segreto professionale forense; segreto professionale medico; **segretezza** delle deliberazioni degli organi giurisdizionali; segretezza derivante da norme di procedura penale, dalla autonomia e indipendenza della magistratura, da esigenze di difesa nazionale e di ordine e sicurezza pubblica, dall'esercizio dei diritti dei lavoratori (diritto di consultare i propri rappresentanti o i sindacati, con garanzia di protezione contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni).

Le informazioni sulle violazioni devono riguardare **comportamenti, atti od omissioni di cui il segnalante o il denunciante sia venuto a conoscenza in un contesto lavorativo pubblico o privato**.

L'accezione da attribuire al **contesto lavorativo** deve necessariamente essere ampia e considerarsi non solo con riguardo a chi abbia un rapporto di lavoro in senso stretto con l'organizzazione del settore pubblico o privato.

Occorre infatti considerare **anche coloro che abbiano instaurato con i soggetti pubblici e privati altri tipi di rapporti giuridici** (consulenti, collaboratori, volontari, tirocinanti, azionisti degli stessi soggetti pubblici e privati ove assumano la forma societaria, persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza). Ciò **anche** quando si tratti di **situazioni precontrattuali**, **periodi di prova o situazioni successive allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso del rapporto stesso**.

Pertanto, a rilevare è l'esistenza di una **relazione qualificata** tra il segnalante e il soggetto pubblico o privato nel quale il primo opera, relazione che riguarda **attività lavorative o professionali presenti o anche passate**.

I **motivi** che hanno indotto la persona a segnalare, denunciare o divulgare pubblicamente sono **irrilevanti** ai fini della trattazione della segnalazione e della protezione da misure ritorsive.

In ogni caso, **non sono considerate segnalazioni di Whistleblowing quelle aventi ad oggetto una contestazione, rivendicazione o richiesta legata ad un interesse di carattere personale del segnalante.**

Le segnalazioni da cui **non** sia **possibile ricavare l'identità del segnalante** sono considerate **anonime**.

I soggetti del settore pubblico e del settore privato che ricevono le segnalazioni tramite canali interni considerano le segnalazioni anonime **alla stregua di segnalazioni ordinarie da trattare secondo i criteri stabiliti nei rispettivi ordinamenti**.

Nei casi di segnalazione, denuncia all'autorità giudiziaria o contabile o divulgazione pubblica anonime, **se la persona segnalante è stata successivamente identificata e ha subito ritorsioni si applicano le misure di protezione per le ritorsioni**.

4 I canali di presentazione delle segnalazioni

Il decreto, nel recepire le indicazioni della Direttiva europea, ha previsto un sistema diversificato di presentazione delle segnalazioni.

L'amministrazione o ente deve approntare canali interni per ricevere e trattare le segnalazioni. Questi canali sono senza dubbio privilegiati, in quanto più prossimi all'origine delle questioni oggetto della segnalazione.

Solo ove si verifichino **particolari condizioni specificamente previste dal legislatore** i segnalanti possono fare ricorso al **canale esterno** attivato **presso ANAC ai sensi degli artt. 5 ss. del D. Lgs. 24/2023**.

Nell'ottica di consentire di scegliere il canale di segnalazione più adeguato in funzione delle circostanze specifiche del caso, è stata prevista anche la possibilità di effettuare una **divulgazione pubblica**, ma in presenza di **particolari condizioni assolutamente residuali e rigidamente disciplinate dall'art. 15 del D. Lgs. 24/2023**

Si deve comunque effettuare una denuncia nei casi in cui il diritto dell'Unione o nazionale **imponga** alle persone segnalanti di rivolgersi alle autorità nazionali competenti, per esempio nell'ambito dei propri **doveri** e **responsabilità professionali** o in ragione del fatto che la violazione possa costituire **reato**.

5 Disciplina organizzativa dei canali di segnalazione interna alla Città Metropolitana di Genova[2]

Con il presente atto organizzativo, Città Metropolitana di Genova intende stabilire:

1. i **canali di segnalazione interna**, previa individuazione dei relativi profili di adeguatezza;
2. il **ruolo ed i compiti** dei soggetti a cui è consentito l'accesso alle informazioni e ai dati contenuti nella segnalazione;
3. **modalità e termini di conservazione dei dati**.

L'art. 4 del D. Lgs. 24/2023 prevede che i soggetti del settore pubblico e i soggetti del settore privato, **sentite le rappresentanze o le organizzazioni sindacali** di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivino propri canali di segnalazione che garantiscano, **anche tramite il ricorso a strumenti di crittografia**, la **riservatezza dell'identità della persona segnalante**, **della persona coinvolta e della persona comunque menzionata nella segnalazione**, nonché **del contenuto della segnalazione e della relativa documentazione**.

La **gestione dei canali di segnalazione interna** è affidata, in ossequio alla previsione contenuta nel comma 5 dell'art. 4 del D.Lgs. 24/2023, al Responsabile Prevenzione Corruzione e Trasparenza (RPCT), il quale può avvalersi di personale espressamente autorizzato a ricevere o a dare seguito alle segnalazioni, ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196. Tale autorizzazione terrà conto del principio del privilegio minimo (PoLP), mutuato dall'ambiente della sicurezza delle informazioni, secondo il quale, ad un utente, vengono concessi i livelli – o permessi – minimi di accesso dei quali ha bisogno per svolgere le proprie mansioni.

Ai sensi di legge, le segnalazioni possono essere effettuate:

- in **forma scritta**, anche con modalità informatiche (piattaforma on line);
- su richiesta della persona segnalante, mediante un **incontro diretto** fissato entro un termine ragionevole.

Al fine di promuovere e valorizzare comportamenti eticamente adeguati da parte del personale aziendale impiegato ad ogni livello negli affidamenti di beni, servizi e lavori, si dispone l'inserimento nei documenti contrattuali dell'**obbligo**, in capo all'**operatore economico**, di rendere nota a **dipendenti e subappaltatori** la procedura del c.d. "Whistleblowing" con **link diretto alla pagina dedicata sul sito internet della Città metropolitana di Genova**.

[2] Si rinvia, ad integrazione della presente parte narrativa, al documento tecnico sulla piattaforma informatica e al diagramma di flusso rappresentativo dell'iter di segnalazione (allegati).

5.1 Tipologie di canale di segnalazione

La Città metropolitana di Genova intende favorire il ricorso all'istituto del whistleblowing, assicurando molteplicità di canali disponibili e adeguate procedure gestionali.

5.1.1 Piattaforma informatica

È istituita e resa disponibile, quale canale di segnalazione e di comunicazione con il segnalante, primariamente consigliato, una piattaforma informatica, raggiungibile via web da chi intenda effettuare una segnalazione, nonché da parte del RPCT e del personale autorizzato. Essa presenta tutte le caratteristiche di sicurezza necessarie a garantire la protezione dell'identità del segnalante e delle altre persone tutelate dalla normativa di riferimento.

La piattaforma, realizzata utilizzando il software open-source "Globaleaks" (https://www.globaleaks.org/it/) è fruibile da tutti i principali browser (Mozilla Firefox, Google Chrome, Brave, Edge, Safari). Si raccomanda l'utilizzo di Tor Browser che protegge l'anonimato degli utenti e include vari miglioramenti della privacy e della sicurezza non presenti in altri browser.

La piattaforma consente l'acquisizione delle segnalazioni che il segnalante intenda effettuare in forma scritta o in modalità orale, mediante registrazione vocale (questa funzione è in via di rilascio da parte degli sviluppatori del software). E' possibile il caricamento di documenti in formato digitale.

La piattaforma informatica dedicata costituisce un registro speciale di protocollazione e consente l'identificazione di ogni segnalazione ricevuta mediante l'attribuzione di un codice univoco progressivo di 16 caratteri (key code), generato in modo casuale e automatico dalla piattaforma stessa.

Si precisa che, in caso di smarrimento del key code, il segnalante non può effettuare l'accesso alla segnalazione. Il key code non può essere replicato. Si rammenta quindi che è onere del segnalante averne adeguata cura. In caso di smarrimento del key code diventa onere del segnalante far presente al RPCT tale situazione, comunicando ogni informazione utile, in merito alla segnalazione di cui ha smarrito il key code.

Una volta effettuato l'accesso alla piattaforma informatica, il segnalante che non intenda rimanere anonimo, inserisce le informazioni che lo identificano univocamente e le informazioni in suo possesso per identificare eventuali altri soggetti citati nella segnalazione.

L'interessato è in ogni caso tenuto a compilare, in modo chiaro, preciso e circostanziato, tutte le sezioni del modulo di segnalazione fornendo le informazioni richieste come obbligatorie e il maggior numero possibile di quelle facoltative.

Il segnalante che abbia inserito la segnalazione tramite piattaforma non può, successivamente, accedere ad essa attraverso altri canali.

Al fine di garantire una più efficace e sicura gestione della segnalazione, ogni qualvolta pervenga una segnalazione a mezzo di un canale diverso dalla piattaforma dedicata, il RPCT invita il segnalante a creare una nuova segnalazione, utilizzando la piattaforma, all'interno della quale annotare l'avvenuta presentazione di una segnalazione attraverso un altro canale.

Ove, a seguito dell'invito ricevuto, il segnalante proceda con l'inserimento della nuova segnalazione, il RPCT (o suo delegato) vi inserisce le informazioni ed i documenti già eventualmente ricevuti attraverso altro canale. Ogni ulteriore attività, quale l'acquisizione di documenti ed informazioni, il caricamento di documenti ed eventuali comunicazioni con il segnalante, avverrà con tale modalità.

Nel caso in cui il segnalante, debitamente invitato, non inserisca una nuova segnalazione sulla piattaforma dedicata, il RPCT (o suo delegato) procederà con la creazione di una segnalazione, qualificata come "interna", nella quale inserire tutte le informazioni ed i documenti acquisiti con altro canale.

L'utilizzo della piattaforma informatica consente al segnalante di accedere alla propria segnalazione fino a cinque anni successivi alla data dell'archiviazione da parte della Città Metropolitana di Genova della segnalazione stessa - tramite l'utilizzo del codice identificativo univoco (key code) che gli viene fornito all'esito della procedura di segnalazione (sia essa anonima o con identificazione) – e di dialogare con Città Metropolitana di Genova. Ciò al fine di monitorare lo svolgimento del procedimento amministrativo eventualmente avviato in seguito alla segnalazione.

Si auspica un comportamento collaborativo del segnalante, al quale si richiede, anche nel proprio interesse, di tenere costantemente aggiornata Città Metropolitana di Genova in ordine all'evoluzione della propria segnalazione/comunicazione, soprattutto quando questa non sia più connotata dal carattere di attualità.

In ragione delle caratteristiche operative e delle misure tecniche ed organizzative adottate, la medesima piattaforma viene altresì individuata quale strumento gestionale di tutta l'attività (istruttoria compresa) compiuta dal RPCT o suo delegato, in relazione alle segnalazioni pervenute, anche se provenienti da canali differenti.

La piattaforma registra le operazioni svolte dal RPCT e dal personale autorizzato, ai fini dell'attribuzione delle responsabilità delle operazioni eseguite.

I soggetti autorizzati ad operare sulla piattaforma, in modalità c.d. back-end sono il RPCT ed i soggetti dal medesimo delegati, con compiti di gestione delle segnalazioni ed il personale tecnico con compiti di amministratore del sistema informatico, non autorizzato ad accedere alle segnalazioni né all'identità del segnalante.

5.1.2 Segnalazioni a mezzo posta o consegna diretta

In alternativa all'utilizzo della piattaforma, il segnalante può ricorrere a forme di comunicazione scritta tradizionali, quali la spedizione a mezzo posta (preferibilmente raccomandata con avviso di ricevimento) o la consegna diretta.

Questa modalità richiede l'adozione di ulteriori accorgimenti da parte del segnalante per garantire la riservatezza dei dati personali, anche in caso di apertura accidentale. E' infatti necessario che vengano utilizzate **tre buste chiuse**:

- **Prima busta**: il segnalante compila ed inserisce il **modulo di segnalazione** con indicati tutti gli elementi essenziali sopra riportati o comunque utili per procedere a verifiche e controlli (modulo disponibile sul sito web istituzionale all'indirizzo: https://www.cittametropolitana.genova.it/it/content/whistleblowing)
- **Seconda busta**: (i) nel caso il segnalante intenda rivelare la propria identità, compila ed inserisce il **modulo con i propri dati identificativi** (modulo disponibile sul sito web istituzionale all'indirizzo: https://www.cittametropolitana.genova.it/it/content/whistleblowing), unitamente alla fotocopia del documento di riconoscimento; (ii) nel caso il segnalante non intenda rivelare la propria identità, inserisce nella busta eventuali modalità con le quali il ricevente potrà comunicare con il segnalante stesso (si veda quanto previsto in relazione all'utilizzo della piattaforma informatica);

- **Terza busta:** il segnalante inserisce le due buste precedentemente preparate (al fine di separare i dati del segnalante dalla segnalazione stessa) e reca, all'esterno, la dicitura "***riservata personale al RPCT di Città Metropolitana di Genova (con indirizzo postale)***", senza indicare in alcun modo sulla busta i propri dati.

Il soggetto ricevente curerà la trasmissione della busta al RPCT, senza aprirla.

La documentazione analogica fatta pervenire dal segnalante è acquisita in modalità digitale per essere registrata all'interno della piattaforma dedicata, sotto la responsabilità del RPCT, il quale assicura che la conservazione analogica avverrà con modalità tali da proteggere l'identità del segnalante e delle altre

persone fisiche che beneficiano della medesima tutela.

Eventuali documenti informatici sono registrati nella piattaforma dedicata ed i supporti, utilizzati per la relativa trasmissione, sono conservati con le stesse modalità della documentazione analogica.

È **escluso l'utilizzo della posta elettronica** quale canale di segnalazione interna.

Non è consentito effettuare una segnalazione utilizzando il tradizionale sistema telefonico. Nessun ufficio è autorizzato a ricevere (e gestire) segnalazioni telefoniche.

5.1.3 Appuntamento con il RPCT

Il segnalante che non intenda avvalersi dei canali di segnalazione di cui sopra, può, con qualsiasi mezzo, analogico o digitale, scritto od orale, **chiedere un incontro diretto** che sarà tenuto entro 30 giorni dalla richiesta, dal RPCT o suo delegato. La richiesta di appuntamento non costituisce segnalazione e non sono raccolte informazioni diverse ed ulteriori rispetto a quelle necessarie alla fissazione e gestione dell'incontro. La documentazione e verbalizzazione della segnalazione orale, resa durante l'incontro, avverrà nel rispetto di quanto previsto dall'art. 14 del D.Lgs. 24/2023.

La verbalizzazione dell'incontro, unitamente alla documentazione analogica eventualmente consegnata dal segnalante è acquisita in modalità digitale per essere registrata all'interno della piattaforma dedicata, sotto la responsabilità del RPCT, il quale assicura che la conservazione analogica avverrà con modalità tali da proteggere l'identità del segnalante e delle altre persone fisiche che beneficiano della medesima tutela.

Eventuali documenti informatici sono registrati nella piattaforma dedicata ed i supporti utilizzati per la relativa trasmissione, sono conservati con le stesse modalità della documentazione analogica.

5.2 Attività di gestione delle segnalazioni

La segnalazione interna presentata ad un soggetto diverso dal RPCT è trasmessa a quest'ultimo, senza ritardo e, comunque, entro sette giorni dal suo ricevimento, dando contestuale notizia della trasmissione alla persona segnalante.
È fatto divieto al ricevente di prendere conoscenza del contenuto della segnalazione (e dell'identità del segnalante) nel caso in cui risulti chiaramente, nell'oggetto della segnalazione o da altri elementi esteriori, che si tratta di una segnalazione per la quale si intende mantenere riservata l'identità del segnalante e beneficiare delle tutele previste nel caso di eventuali ritorsioni subite in ragione della segnalazione.
Nell'ambito della gestione del canale di segnalazione interna, il RPCT e il soggetto appositamente autorizzato (di seguito: Delegato), ai quali è affidata la gestione diretta del canale di segnalazione interna svolgono le seguenti attività:

1. rilasciano alla persona segnalante **avviso di ricevimento** della segnalazione **entro sette giorni** dalla data di ricezione;
2. mantengono le **interlocuzioni** con la persona segnalante e possono richiedere a quest'ultima, se necessario, **integrazioni**;
3. danno **diligente seguito** alle segnalazioni ricevute;
4. forniscono **riscontro alla segnalazione entro 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;
5. mettono a disposizione informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne (sito *internet* e *intranet*)

In particolare, il "diligente 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.

In 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 e comunque laddove quanto segnalato non sia adeguatamente circostanziato, il RPCT, anche tramite Delegato, 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 a titolo di *whistleblowing*, il RPCT avvia, con il supporto del Delegato, l'istruttoria interna sui fatti o sulle condotte segnalate, ponendo in essere gli atti necessari ad una imparziale valutazione circa la sussistenza di quanto oggetto di segnalazione. Ove necessario, il RPCT e il Delegato possono anche acquisire atti e documenti da altri uffici dell'amministrazione, avvalersi del loro supporto, coinvolgere terze persone tramite audizioni e altre richieste, avendo sempre cura che non sia compromessa la riservatezza dei soggetti tutelati dal d. lgs. 24/2023.

Il RPCT che constati essere stati raccolti dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione ne dispone l'immediata cancellazione o distruzione, annotando la categoria dei dati e le ragioni della ritenuta non utilità.

Qualora il RPCT ritenga di consultare altri uffici interni all'Amministrazione, per svolgere l'attività di verifica e di analisi della segnalazione, egli stesso ha cura di formulare le richieste in modo tale da non rendere possibile che esse siano riconducibili a soggetti specifici appositamente tutelati dalla norma citata.

Al fine di garantire la riservatezza dei soggetti che beneficino della tutela normativa prevista dal D. Lgs.24/2023, la loro identità potrà essere conosciuta solo dal RPCT e, su sua disposizione, dal Delegato.

Pertanto, all'esito dell'istruttoria, il RPCT, anche tramite Delegato, fornisce riscontro alla segnalazione, esplicitando le misure previste o adottate o da adottare e le relative motivazioni, 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.

Qualora la segnalazione sia ritenuta fondata, il RPCT si rivolge agli organi preposti interni o agli enti o alle istituzioni esterne, secondo le rispettive competenze.
Il RPCT può invece disporre l'archiviazione della segnalazione, con adeguata motivazione, laddove la stessa sia ritenuta manifestamente infondata.

5.3 Comunicazione con il segnalante ed acquisizione di documenti ed informazioni

Qualora il segnalante abbia effettuato la segnalazione attraverso la piattaforma dedicata, le comunicazioni e l'acquisizione di documenti ed informazioni avvengono per il tramite della piattaforma medesima.

Nel caso in cui il segnalante abbia effettuato la segnalazione avvalendosi di canali diversi dalla piattaforma dedicata, le comunicazioni e l'acquisizione di documenti ed informazioni avvengono utilizzando il canale scelto dal segnalante, tenuto comunque conto di quanto previsto al par. 4

5.4 Segnalazioni anonime

Le segnalazioni da cui non sia possibile ricavare l'identità del segnalante sono considerate anonime.

Le segnalazioni anonime sono prese in considerazione solo ove si presentino adeguatamente circostanziate e sono rese con dovizia di particolari, in modo da far emergere fatti e situazioni connessi a contesti determinati.

Le segnalazioni anonime e la relativa documentazione sono conservate per cinque anni, decorrenti dalla data di ricezione.

5.5 Protezione dei dati personali

L'assolvimento degli obblighi previsti dal D.Lgs. 24/2023 comporta il trattamento di dati personali, riguardanti le persone fisiche che beneficiano della tutela normativa nonché di quelle coinvolte nell'attività di gestione delle segnalazioni.

Rispetto a tali trattamenti Città Metropolitana di Genova, nella qualità di Titolare del trattamento, ha definito il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del RGPD.

La scelta dei canali di segnalazione interna e la predisposizione delle misure tecniche ed organizzative ha visto il coinvolgimento del Responsabile della Protezione dei Dati Personali (RPD o DPO), il quale ha altresì espresso parere favorevole alle conclusioni contenute nella DPIA.

Sarà cura dell'Amministrazione garantire che gli interessati ricevano le informazioni di cui agli articoli 13 e 14 del RGPD, secondo criteri di tempestività ed adeguatezza, privilegiando la modalità digitale.

È istituita, all'interno del sito web istituzionale dell'Ente, apposita pagina dedicata all'istituto del whistleblowing, presso la quale sono rese disponibili informazioni dettagliate circa i canali a disposizione per inviare segnalazioni alla civica amministrazione, il collegamento alla piattaforma informatica dedicata ed il collegamento ai canali di segnalazione esterni individuato da ANAC.

6 Denuncia all'Autorità giurisdizionale

Il decreto, in conformità alla precedente disciplina, riconosce ai soggetti tutelati anche la possibilità di valutare di rivolgersi alle Autorità nazionali competenti, giudiziarie e contabili, per inoltrare una denuncia di condotte illecite di cui questi siano venuti a conoscenza in un contesto lavorativo pubblico o privato.

ANAC richiama l'attenzione sui seguenti punti:

- qualora il whistleblower rivesta la **qualifica di pubblico ufficiale o di incaricato di pubblico servizio**, anche laddove lo stesso abbia effettuato una segnalazione attraverso i canali interni o esterni previsti dal decreto, ciò non lo esonera dall'**obbligo** - in virtù di quanto previsto dal combinato disposto dell'art. 331 c.p.p. e degli artt. 361 e 362 c.p - **di denunciare alla competente Autorità giudiziaria o contabile i fatti penalmente rilevanti e le ipotesi di danno erariale**;
- in ogni caso l'ambito oggettivo degli artt. 361 e 362 c.p., disponendo l'obbligo di denunciare soltanto **reati (procedibili d'ufficio)**, è più ristretto di quello delle segnalazioni effettuabili dal *whistleblower* che può segnalare anche illeciti di altra natura;
- laddove il dipendente pubblico denunci un reato all'Autorità giudiziaria ai sensi degli artt. 361 o 362 c.p. e poi venga discriminato per via della segnalazione, potrà beneficiare delle tutele previste dal decreto per le ritorsioni subite;
- le stesse regole sulla tutela della riservatezza e del contenuto delle segnalazioni vanno rispettate dagli uffici delle Autorità giurisdizionali cui è sporta la denuncia.

7 Il sistema delle tutele

Il sistema di tutele previsto dal d.lgs. n. 24/2023 si articola come segue:

1. tutela della **riservatezza** del segnalante, del facilitatore, della persona coinvolta e delle persone menzionate nella segnalazione (il decreto sancisce espressamente che le segnalazioni non possono

essere utilizzate oltre quanto necessario per dare alle stesse adeguato seguito);

2. la tutela **da** eventuali **misure ritorsive** adottate dall'ente in ragione della segnalazione, divulgazione
3. pubblica o denuncia effettuata e le condizioni per la sua applicazione;
4. le **limitazioni della responsabilità** rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni che operano al ricorrere di determinate condizioni;
5. la previsione di **misure di sostegno** da parte di enti del Terzo settore inseriti in un apposito elenco pubblicato da ANAC;
6. **divieto di rinunce e transazioni**, non sottoscritte in sede protetta ex art. 2113 c.4 del codice civile, dei diritti e dei mezzi di tutela previsti.

Dalla tutela della identità del segnalante deriva indirettamente un *favor*, riconosciuto da questa Amministrazione, nei confronti della gestione informatizzata delle segnalazioni, con il ricorso a strumenti di crittografia, oltre alla sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso agli atti amministrativi.

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 effettuate in forma orale a seguito un incontro diretto con chi tratta la segnalazione.

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 segnalazione interna, laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta.

L'obbligo di tutelare la riservatezza impone che un eventuale disvelamento dell'identità della persona segnalante a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni avvenga sempre con il **consenso espresso** della stessa.

Il divieto di rivelare l'identità del segnalante è da riferirsi non solo al nominativo del segnalante ma anche a **qualsiasi altra informazione o elemento della segnalazione, ivi inclusa la documentazione ad essa allegata**, dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante.

Nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell'ambito dei canali interni di segnalazione, è di regola da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al predetto principio di integrità e riservatezza. Le misure di sicurezza adottate devono, comunque, essere periodicamente riesaminate e aggiornate.

Da ultimo, si ricorda che la persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, divulgazione pubblica o denuncia, non possono esercitare i diritti che normalmente il GDPR riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento). Ciò in quanto dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della

riservatezza dell'identità della persona segnalante. In tali casi, dunque, al soggetto segnalato o alla persona menzionata nella segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali.

Il decreto prevede, a tutela del whistleblower, il **divieto di ritorsione** definita come *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*.

Si tratta quindi di una definizione ampia del concetto di ritorsione che può consistere sia in atti o provvedimenti ma anche in comportamenti od omissioni che si verificano nel contesto lavorativo e che arrecano pregiudizio ai soggetti tutelati. In discontinuità con il passato, invece, il d.lgs. n. 24/2023 nel fornire una definizione di ritorsione vi include anche quelle *solo tentate o minacciate*.

Affinché si possa configurare una ritorsione e, di conseguenza, il soggetto possa beneficiare di protezione è necessario uno stretto collegamento tra la segnalazione, la divulgazione e la denuncia e il comportamento, atto, omissione sfavorevole subiti, direttamente o indirettamente, dalla persona segnalante, denunciante o che effettui la divulgazione pubblica.

L'elencazione delle ritorsioni da parte del legislatore è molto più ampia rispetto alla precedente disciplina, pur tuttavia con carattere non tassativo.

ANAC riconduce all'insieme delle tutele, riconosciute dalla disciplina al segnalante, denunciante o a chi effettua una divulgazione pubblica, anche le **limitazioni della responsabilità rispetto alla rivelazione e alla diffusione di alcune categorie di informazioni**. Si tratta di limitazioni che operano al ricorrere di determinate condizioni, in assenza delle quali vi sarebbero conseguenze in termini di responsabilità penale, civile, amministrativa. Il segnalante deve agire per tutelare l'interesse all'integrità delle amministrazioni, pubbliche e private, e per prevenire e reprimere le malversazioni. Inoltre egli non deve aver appreso la notizia in ragione di un rapporto di consulenza professionale o di assistenza con l'ente, l'impresa o la persona fisica interessata.

Le notizie e i documenti, oggetto di segreto aziendale, professionale o d'ufficio, non devono essere rivelati con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in particolare, la rivelazione non deve avvenire al di fuori del canale di comunicazione specificamente predisposto per le segnalazioni.

Ad ulteriore rafforzamento della protezione del segnalante il legislatore per la prima volta prevede la possibilità che **ANAC stipuli convenzioni con enti del Terzo settore** affinché questi ultimi forniscano misure di sostegno al segnalante. In particolare tali enti, **inseriti in un apposito elenco pubblicato da ANAC sul proprio sito istituzionale**, prestano **assistenza e consulenza a titolo gratuito**:

- ✓ sulle modalità di segnalazione;
- ✓ sulla protezione dalle ritorsioni riconosciuta dalle disposizioni normative nazionali e da quelle dell'Unione europea;
- ✓ sui diritti della persona coinvolta.

Il d.lgs. n. 24/2023 disciplina, infine, le **comunicazioni ad ANAC delle ritorsioni** che i soggetti ritengano di aver subito a causa della segnalazione, denuncia o divulgazione pubblica effettuata.

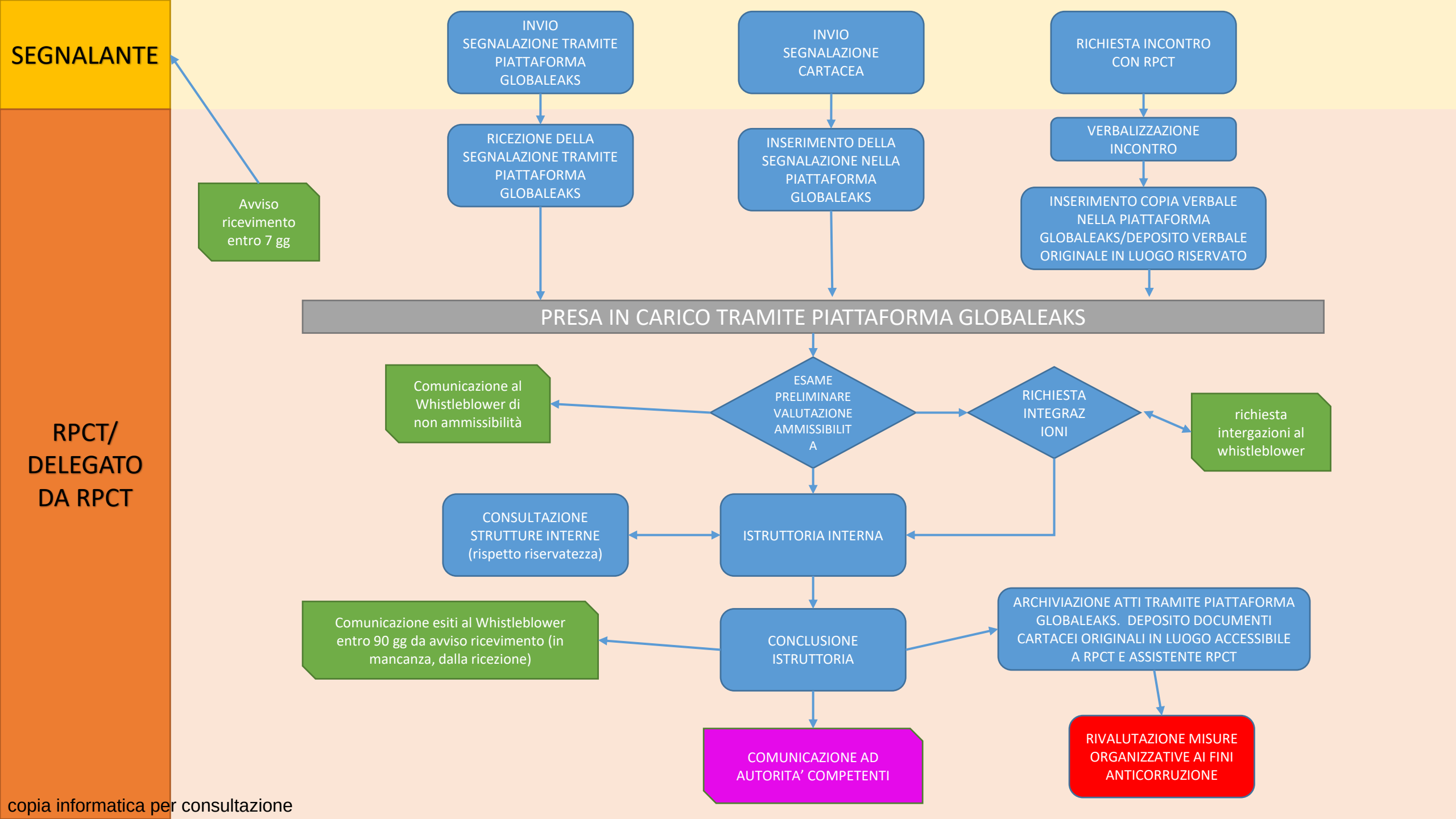
La nuova disciplina include, tra i soggetti che possono effettuare la comunicazione ad ANAC, anche coloro che, a fronte di un legame qualificato con il segnalante, denunciate o divulgatore pubblico, subiscano ritorsioni in ragione di detta connessione (facilitatori, persone del medesimo contesto lavorativo, colleghi di lavoro, e anche soggetti giuridici nei casi in cui siano enti di proprietà del segnalante, denunciate, divulgatore pubblico o enti in cui lavora o enti che operano nel medesimo contesto lavorativo).

In discontinuità con la precedente normativa, sono **escluse dal diritto di comunicare ad ANAC la ritorsione**, le **organizzazioni sindacali** maggiormente rappresentative nell'amministrazione/ente in cui le ritorsioni siano state poste in essere. I rappresentanti sindacali hanno comunque la possibilità di comunicare ad ANAC ritorsioni, sia se esse sono conseguenza di una segnalazione, denuncia, divulgazione pubblica dagli stessi effettuata in qualità di lavoratori, sia se assumano il ruolo di facilitatori, non spendendo la sigla sindacale: la ritorsione potrebbe infatti derivare dall'aver fornito consulenza e sostegno alla persona segnalante, denunciate o che abbia effettuato una divulgazione pubblica

È sempre necessario che il segnalante fornisca ad ANAC **elementi oggettivi** dai quali sia possibile dedurre la consequenzialità tra segnalazione, denuncia, divulgazione pubblica effettuata e la lamentata ritorsione.

Il decreto prevede che **le comunicazioni di ritorsioni siano trasmesse esclusivamente ad ANAC per gli accertamenti che la legge le attribuisce e per l'eventuale irrogazione della sanzione amministrativa al responsabile. È necessario, quindi, che i soggetti del settore pubblico e privato forniscano chiare indicazioni sul sito istituzionale a riguardo, affinché le comunicazioni siano correttamente inoltrate ad ANAC.**

In ogni caso, i soggetti pubblici o privati che per errore fossero destinatari di una comunicazione di ritorsione sono tenuti a garantire la riservatezza dell'identità della persona che l'ha inviata e a trasmetterla ad ANAC, dando contestuale notizia di tale trasmissione al soggetto che abbia effettuato la comunicazione.



IL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati – di seguito, RGPD);

VISTO il d.lgs. 30 giugno 2003, n. 196, recante "Codice in materia di protezione dei dati personali" (di seguito, Codice privacy);

VISTA la 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 (c.d. "whistleblowing") (di seguito, Direttiva);

VISTO il parere del Garante sullo schema di decreto legislativo recante attuazione della Direttiva, adottato con provvedimento dell'11 gennaio 2023, n. 1 (doc. web n. 9844945);

VISTO il d.lgs. 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*
- di seguito, Decreto), con il quale la Direttiva è stata recepita nell'ordinamento interno;

CONSIDERATO che il Decreto assicura nell'ordinamento interno la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato (art. 1, comma 1, del Decreto);

CONSIDERATO, altresì, che le condotte o le omissioni oggetto di segnalazione possono consistere, in particolare, in violazioni del diritto nazionale (illeciti civili, illeciti amministrativi, illeciti penali, illeciti contabili, condotte illecite rilevanti ai sensi del d.lgs.
n. 231/2001, violazioni dei modelli di organizzazione e gestione previsti nel d.lgs. n. 231/2001), nonché in violazioni della normativa dell'Unione europea indicata nell'Allegato 1 al Decreto e di tutte le disposizioni nazionali che ne danno attuazione e che, in tale ambito, sono indicate anche le disposizioni a "*tutela della vita privata e dei dati personali e sicurezza delle reti e dei sistemi informativi*", (art. 2, comma 1, lett. a), nn. 1-6, e lett. J) All. 1 del Decreto, con specifico riferimento al Regolamento e al Codice);

CONSIDERATO che la persona segnalante è, in base a tale disciplina di settore, la persona fisica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo (art. 2, co. 1, lett. g), del Decreto), ovvero nel contesto delle attività lavorative o professionali, presenti o passate, nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile (art. 2, comma 1, lett. i), del Decreto);

CONSIDERATO che la tutela approntata dal Decreto si applica non solo se la segnalazione, la denuncia o la divulgazione pubblica avvenga in costanza del rapporto di lavoro o di altro tipo di rapporto giuridico, ma anche anteriormente o successivamente alla costituzione del rapporto giuridico e, in particolare, se le informazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali, o durante il periodo di prova, nonché successivamente allo scioglimento del rapporto giuridico se le informazioni sulle violazioni sono state acquisite nel corso dello stesso (art. 3, comma 4, del Decreto);

VISTO quanto disposto dal Decreto, con particolare riguardo a:

- l’ambito di applicazione soggettivo (art. 3);
- i soggetti del settore pubblico e privato obbligati ad attivare canali di segnalazione interna, i quali devono garantire, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione (art. 4);
- le garanzie a tutela dell’identità del segnalante e della riservatezza degli interessati, anche con riguardo alla necessità che i dati siano trattati da personale espressamente autorizzato ai sensi degli articoli 29 e 32, par. 4, del Regolamento e dell'articolo 2-*quaterdecies* del Codice, nonché che la segnalazione sia sottratta all'accesso previsto dagli artt. 22 e ss. della l. 7 agosto 1990, n. 241, e dagli artt. 5 e ss. del d.lgs. 14 marzo 2013, n. 33 (art.
  12);
- le specifiche garanzie in materia di trattamento dei dati personali, applicabili nell’ambito dell’acquisizione e gestione delle segnalazioni e, in particolare, la cancellazione dei dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione; la limitazione dei diritti di cui agli articoli da 15 a 22 del RGPD, nei limiti di quanto previsto dall' articolo 2-*undecies* del Codice; il ruolo di titolari del trattamento dei soggetti pubblici e privati in relazione ai trattamenti connessi al ricevimento e alla gestione delle segnalazioni e la necessità di assicurare il rispetto dei princìpi generali in materia di protezione dei dati, nonché di adottare misure appropriate a tutela dei diritti e delle libertà degli interessati, fornendo, altresì, l’informativa sul trattamento dei dati personali agli stessi; la possibilità per i titolari del trattamento pubblici e privati di condividere le risorse per il ricevimento e la gestione delle segnalazioni, a condizione di determinare in maniera trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, agendo in qualità di contitolari del trattamento; la necessità che i titolari del trattamento pubblici e privati definiscano il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che, in qualità di responsabili del trattamento, trattano dati personali per loro conto (art. 13);
- il periodo di conservazione della documentazione inerente alle segnalazioni interne ed esterne per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione nonché le modalità anche informatiche di ricezione delle segnalazioni, ovvero oralmente anche attraverso una linea telefonica registrata, un sistema di messaggistica vocale registrato o nel corso di un incontro con il personale autorizzato (art. 14);
- le condizioni al ricorre delle quali le persone fisiche possono beneficiare delle misure di protezione previste dalla legge (art. 16);
- il divieto di atti ritorsivi nei confronti del segnalante e degli altri soggetti cui la legge ha esteso tale garanzia (quali, in particolare, facilitatori, persone legate al segnalante da stabile rapporto affettivo o di parentela, colleghi di lavoro) (art. 17);
- la limitazione della responsabilità del segnalante (art. 20) l’invalidità di rinunce e transazioni che hanno per oggetto i diritti riconosciuti dal Decreto (art. 22);
- le norme transitorie e l’abrogazione delle disposizioni di cui all' articolo 54- *bis* del d.lgs. 30 marzo 2001 n. 65, l'art. 6, commi 2-*ter* e 2-*quater*, del d.lgs. 8 giugno 2001, n. 231 e l'art. 3 della l. 30 novembre 2017, n. 179 (art. 23 e

24);

VISTA la nota con la quale il Titolare ha trasmesso al RPD la bozza di DPIA e dello schema di atto organizzativo;

CONSIDERATO che l'acquisizione e gestione delle segnalazioni dà luogo a trattamenti di dati personali, anche appartenenti a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti a interessati (persone fisiche identificate o identificabili) e, in particolare, i segnalanti o le persone indicate come possibili responsabili delle condotte illecite o quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento);

RITENUTO che i trattamenti di dati personali posti in essere dal Titolare, nell'ambito della gestione del canale di segnalazione interno, sono necessari per dare attuazione agli obblighi di legge e ai compiti d'interesse pubblico previsti dalla disciplina di settore la cui osservanza è condizione di liceità del trattamento (artt. 6, par. 1, lett. c) ed e) e parr. 2 e 3, 9, par. 2, lett. b) e g), 10 e 88 del RGPD, nonché 2-*ter* e 2-*sexies* del Codice privacy);

RITENUTO, in ogni caso, che il Titolare del trattamento è tenuto a rispettare non solo le richiamate diposizioni di settore che come detto costituiscono la base giuridica dei relativi trattamenti, ma anche i principi in materia di protezione dei dati (art. 5 del RGPD) e che tale soggetto, nell'ambito della necessaria individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi per gli interessati nel delicato contesto in esame, devono definire il proprio modello di gestione delle segnalazioni in conformità ai principi della "*protezione dei dati fin dalla progettazione*" e della "*protezione per impostazione predefinita*"(artt. 5, par. 1, e par. 2 , 24, 25 e 32 del Regolamento) tenuto conto anche delle osservazioni presentate al riguardo dal responsabile della protezione dei dati (RPD);

CONSIDERATO che il Titolare ha attivato, predisponendo una specifica piattaforma informatica, un canale per le segnalazioni interne che garantisce, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione (ferma restando la possibilità di presentare una segnalazione anche nel corso di incontri in presenza con il personale autorizzato);

CONSIDERATO, più nel dettaglio, che l'impianto procedurale attivato dal Titolare tiene conto delle indicazioni fornite dal Garante per la Protezione dei Dati Personali, in particolare, con riguardo a:

- la possibilità che, anche in caso di segnalazioni prive di dati anagrafici del segnalante, quest'ultimo possa essere, in talune circostanze, identificabile da elementi di contesto, con la conseguenza che tali segnalazioni non possono essere considerate anonime in senso tecnico e sprovviste delle garanzie previste dalla legge;
- la necessità di invitare i segnalanti a utilizzare esclusivamente i canali appositamente istituiti per presentare segnalazioni, considerato che tali canali offrono maggiori garanzie in termini di sicurezza e riservatezza, sebbene anche nell'eventualità in cui una segnalazione sia inviata per errore mediante canali alternativi, debba comunque essere assicurata la riservatezza dell'identità del segnalante e la protezione dei dati di tutti gli interessati;
- la necessità di chiarire che, nell'ambito delle valutazioni funzionali a garantire la scelta del segnalante in merito ai diversi canali di segnalazione (modalità informatiche o canali tradizionali), il ricorso alla posta elettronica ordinaria e certificata non è di per sé adeguato a garantire la riservatezza, e che, quando si utilizzino canali e tecniche tradizionali, occorre indicare gli strumenti previsti per garantire la riservatezza richiesta dalla normativa, assicurando la protocollazione

riservata, ad esempio mediante il meccanismo delle due buste chiuse;

- la puntuale definizione di casi in cui il segnalato può - nel corso dei procedimenti eventualmente avviati nei suoi confronti a seguito della conclusione dell'attività di verifica e di analisi della segnalazione -, essere informato dell'esistenza di una segnalazione che lo riguarda; ciò in quanto nell'ambito dei procedimenti, anche disciplinari, conseguenti alla segnalazione, la contestazione potrebbe essere "*fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa*" (art. 12, comma 5, del Decreto), non essendo, pertanto, necessario che, fuori dei casi espressamente previsti dalla legge al predetto comma 5 (contestazione fondata in tutto o in parte sulla segnalazione; conoscenza dell'identità indispensabile per la difesa; consenso espresso del segnalante), il segnalato venga a conoscenza della circostanza che l'accertamento ha avuto origine da una segnalazione;
- la necessità di considerare quali soggetti autorizzati al trattamento soltanto le persone che, in base alle scelte organizzative del titolare del trattamento, siano competenti a ricevere o a dare seguito alle segnalazioni e siano adeguatamente istruiti al riguardo;
- l'opportunità di chiarire che i titolari del trattamento devono rendere *ex ante* un'informativa sul trattamento dei dati personali ai possibili interessati (segnalanti, segnalati, persone interessate dalla segnalazione, facilitatori, ecc.) mediante la pubblicazione di documenti informativi (ad esempio tramite sito *web* o piattaforma informatica) o per mezzo di informative brevi in occasione dell'utilizzo degli altri canali previsti dal decreto, non dovendo, invece, fornite agli specifici interessati direttamente coinvolti menzionati da una segnalazione informative su base individuale;
- l'opportunità di chiarire che, considerato che il trattamento dei dati personali mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati – in ragione anche della particolare delicatezza delle informazioni potenzialmente trattate, della vulnerabilità degli interessati nel contesto lavorativo, nonché dello specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore – e come espressamente previsto dal Decreto (art. 13, co. 6), i titolari del trattamento devono definire "*il proprio modello di ricevimento e gestione delle segnalazioni* […] *sulla base di una valutazione d'impatto sulla protezione dei dati*";
- l'arco temporale durante il quale occorre garantire la riservatezza del segnalante e degli altri interessati, con particolare riguardo alla circostanza che, stante l'obbligo di conservare la segnalazione non oltre cinque anni a decorrere dalla data dell'esito finale della procedura di segnalazione (art. 14, comma 1, del Decreto), la riservatezza dovrà essere sempre garantita durante tale periodo (fatte salve le ipotesi previste dall'art. 12, commi 3-5, del Decreto), e che, decorso tale periodo, dovendo la segnalazione essere cancellata, verrebbe comunque meno la possibilità di risalire all'identità del segnalante;
- l'opportunità di chiarire che, nell'ottica di privilegiare la volontà del segnalante, è sempre possibile per quest'ultimo ritirare la segnalazione mediante apposita comunicazione da trasmettere attraverso il canale originariamente prescelto per l'inoltro della stessa, specificando le conseguenze derivanti da tale scelta in merito alla prosecuzione o meno degli accertamenti eventualmente già avviati;
- l'opportunità di chiarire, nel caso in cui sia palese l'assoluta irrilevanza rispetto alla vicenda segnalata di parti della segnalazione, che contengono dati personali, le modalità con le quali è possibile assicurare la cancellazione dei dati prevista dall'art. 13, comma 2, del Decreto;

RITENUTO, altresì, che, con riferimento ai profili relativi alla sicurezza del trattamento,

nell’ambito dell’acquisizione e gestione delle segnalazioni tramite piattaforma informatica:

- sono state adottate misure tecniche e organizzative tali da garantire un'adeguata sicurezza del trattamento dei dati personali, compresa la protezione da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali, fermo restando che tali misure saranno, comunque, periodicamente riesaminate e aggiornate;
- nel contesto in esame, caratterizzato da elevati rischi per i diritti e le libertà degli interessati, il ricorso a strumenti di crittografia nell’ambito del canale interno è da ritenersi una misura adeguata a dare attuazione, fin dalla progettazione e per impostazione predefinita, al principio di integrità e riservatezza, garantendo la tutela dei dati personali trattati nel processo di segnalazione, sia nella fase di trasmissione che di conservazione;
- nel caso in cui l’accesso al canale interno di segnalazione avvenga dalla rete dati interna del soggetto obbligato, è garantita la non tracciabilità del segnalante nel momento in cui viene stabilita la connessione a tale canale, sia sulla piattaforma informatica che negli apparati (es. firewall o proxy) eventualmente coinvolti nella trasmissione delle comunicazioni del segnalante;
- sia effettuato, ove possibile, il tracciamento delle operazioni svolte dal personale autorizzato alla gestione delle segnalazioni, nel rispetto delle garanzie a tutela del segnalante e degli altri soggetti menzionati, al fine di consentire la verifica della liceità e correttezza del trattamento e garantire la sicurezza del trattamento (parte prima, par. 4.1.3), nel rispetto delle garanzie previste dalla disciplina di settore in materia di controlli a distanza (art. 4 della l. n. 300/1970, nonché art. 114 del Codice; v. anche art. 88 del Regolamento);

RITENUTO di non dover formulare osservazioni sulla bozza di Atto organizzativo, atteso che le indicazioni fornite in precedenza dal sottoscritto RPD sono state tenute in debita considerazione;

VISTA la documentazione in atti;

TUTTO CIÒ PREMESSO, IL RPD

ai sensi dell’articolo 39, paragrafo 1, lett. C) del RGPD, esprime parere favorevole sulla valutazione d’impatto sulla protezione dei dati personali, condotta dall’Amministrazione la quale conclude nel senso di ritenere “possibile procedere con l’attivazione dei canali di segnalazione interni e l'avvio del trattamento senza ulteriori misure tecniche e organizzative”.

Documento sottoscritto digitalmente