

FOCUS

*Whistleblowing:
linee guida Anac e aspetti operativi*

*Whistleblowing:
Anac guidelines and operational aspects*



PREMESSA

Lo scorso 10 marzo 2023 il Governo ha emanato un decreto che disciplina in modo organico “la protezione delle persone che segnalano violazioni del diritto dell’Unione” e “violazioni di disposizioni normative nazionali” (D. Lgs. n. 24/2023, di seguito anche “il Decreto”).

È noto come la novella legislativa abbia sollevato – e tutt’ora sollevi – molteplici quesiti interpretativi e altrettanti problemi applicativi, cui – da più parti – si è tentato di trovare adeguate soluzioni. Del resto, le società sono chiamate ad un’opera di complesso adattamento alla nuova normativa in materia di *whistleblowing*, pena l’imposizione di sanzioni amministrative pecuniarie la cui entità – a differenza di molti altri temi regolamentati dal Decreto – è stata sin da subito *crystal clear*.

In questo scenario, di particolare rilievo e supporto per le imprese sono le Linee Guida adottate da ANAC con delibera n. 311 del 12 luglio 2023, cui si farà costante riferimento nel prosieguo del *Focus*. Il presente contributo (pagine 2 – 8) – sulla base dell’esperienza già maturata nell’implementazione della materia e senza alcuna pretesa di esaustività – si propone di:

- offrire concrete soluzioni applicative agli interrogativi posti dalla disciplina;
- tracciare una *road map* degli adempimenti che le aziende sono tenute ad effettuare per conformarsi alla nuova normativa.

*

INTRODUCTION

On 10 March 2023, the Government issued a decree that comprehensively regulates “the protection of persons who report breaches of Union law” and “breaches of national legislation” (Legislative Decree No. 24/2023, hereinafter ‘*the Decree*’).

It is well known that the new legislation raised - and still raises today - many questions of interpretation and as many application problems, to which - from several sides - attempts have been made to find adequate solutions. Moreover, companies are called upon to make a complex adjustment to the new *whistleblowing* legislation, to avoid the imposition of administrative fines, the extent of which - unlike many other issues regulated by the Decree - has been crystal clear from the outset.

In this scenario, of particular importance and support for companies are the Guidelines adopted by ANAC with Resolution No. 311 of 12 July 2023, to which constant reference will be made in the remainder of this *Focus*. This contribution (pages 9 - 15) - on the basis of the experience already gained in the implementation of the matter and without any claim to exhaustiveness - aims to:

- offer concrete application solutions to the questions posed by the discipline;
- outline a *road map* of what companies are required to do to comply with the new legislation.

I. A QUALI SOGGETTI SI APPLICA LA NUOVA DISCIPLINA E A PARTIRE DA QUANDO?

Tra gli altri, il Decreto ha sicuramente il pregio di aver definito con chiarezza l'ambito soggettivo di applicazione della nuova disciplina.

Oltre agli enti del settore pubblico, sono destinatari della normativa *Whistleblowing*:

- gli enti che hanno impiegato nell'ultimo anno una media di **almeno cinquanta lavoratori subordinati** (con contratti a tempo determinato o indeterminato);
- gli enti che operano in **specifici settori** (bancario, del credito, dell'investimento, dell'assicurazione e della riassicurazione, delle pensioni professionali o dei prodotti pensionistici individuali, dei titoli, dei fondi di investimento, dei servizi di pagamento) ancorché con una media di lavoratori inferiore a cinquanta nell'ultimo anno;
- gli enti che abbiano adottato **Modelli organizzativi e di gestione** ai sensi del D. Lgs. n. 231/2001 (di seguito anche "*Modelli 231*"), ancorché con una media di lavoratori inferiore a cinquanta nell'ultimo anno.

Ai fini del calcolo della media annua dei lavoratori impiegati, ciascun ente deve fare riferimento – di volta in volta – all'ultimo anno solare precedente a quello in corso, salvo per le imprese di nuova costituzione, per le quali si considera l'anno in corso.

Sempre con riferimento al settore privato, le disposizioni transitorie scandiscono cronologicamente l'efficacia delle disposizioni del Decreto, chiarendo che esse hanno effetto:

- **a partire dal 15 luglio 2023**, per gli enti che hanno impiegato una media di almeno 250 lavoratori subordinati (con contratti di lavoro a tempo indeterminato o determinato) nell'ultimo anno;
- **a partire dal 17 dicembre 2023**, per gli enti che hanno impiegato una media di lavoratori subordinati inferiore a 250 nell'ultimo anno.

II. COSA PUÒ ESSERE OGGETTO DI SEGNALAZIONE NEGLI ENTI CHE OCCUPANO MENO DI 50 DIPENDENTI?

Nell'ambito degli enti che occupino meno di 50 dipendenti e che abbiano adottato Modelli 231, potranno essere effettuate segnalazioni di condotte che integrino reati presupposto della disciplina di cui al D. Lgs. 231/2001 o violazioni del Modello. Dette segnalazioni possono essere effettuate esclusivamente tramite il canale interno istituito dall'ente.

Diversamente, negli enti che occupino meno di 50 dipendenti, ma operino in uno dei settori elencati dal Decreto – come sopra individuati – potranno invece essere effettuate anche segnalazioni di violazioni di disposizioni dell'Unione Europea, attraverso tutti i canali di segnalazione.

Naturalmente, tale possibilità è prevista anche per gli enti che occupino più di 50 dipendenti.

III. COSA DEVONO FARE GLI ENTI ENTRO LE CITE SCADENZE?

Gli adempimenti cui gli enti sopra individuati devono – tempestivamente – provvedere si possono riassumere nella seguente *road map*:

1. individuazione del gestore delle segnalazioni (interno o esterno, monocratico o collegiale);
2. individuazione del canale di segnalazione interno;
3. adozione di una *policy whistleblowing*;
4. aggiornamento del Modello 231, del Codice Etico e della eventuale documentazione interna che menzioni i canali di segnalazione;
5. adempimenti relativi alla *privacy*;
6. informazione nei confronti di soggetti interni ed esterni all'organizzazione;
7. formazione dei dipendenti e del gestore, se interno.

In primo luogo, ciascun ente deve provvedere alla adozione di una *policy* che regolamenti integralmente la materia *whistleblowing* all'interno della medesima realtà organizzativa.

È opportuno che tale attività sia affidata ad un legale o – ad ogni modo – ad un soggetto qualificato e dotato di competenze specifiche in materia, eventualmente esterno all'ente.

In modo particolare, la *policy* deve:

- definire il ruolo e i compiti dei soggetti preposti alla gestione delle segnalazioni;
- individuare le modalità e i termini di conservazione dei dati;
- prevedere e regolamentare diverse modalità di segnalazione (in forma scritta e orale);

- prevedere procedure che garantiscano la riservatezza del segnalante, degli altri soggetti indicati dal Decreto e del contenuto della segnalazione;
- prevedere iniziative di sensibilizzazione e formazione del personale per divulgare le finalità dell'istituto del *whistleblowing* e la procedura per il suo utilizzo.

Parallelamente, gli enti del settore privato che abbiano adottato Modelli 231 dovranno procedere all'**aggiornamento dei Modelli**: il Decreto ha infatti previsto che siano questi ultimi a disciplinare i canali di segnalazione interna, il divieto di ritorsione ed il sistema disciplinare. Alternativamente, il Modello 231 dovrà contenere un esplicito rinvio alla *policy*.

IV. CANALE INTERNO: QUALI MODALITÀ DI SEGNAZIONE DEVE PREVEDERE LA POLICY?

Il Decreto richiede che ciascun ente preveda, in via alternativa, due diverse modalità di acquisizione delle segnalazioni: in forma scritta ("*anche con modalità informatiche*") e in forma orale ("*attraverso linee telefoniche o con sistemi di messagistica orale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole*").

Unico – e imprescindibile – requisito è quello che i canali garantiscano, "*anche mediante il ricorso a strumenti di crittografia*", la riservatezza:

- del segnalante;
- del facilitatore;
- della persona coinvolta o della persona comunque menzionata nella segnalazione;
- del contenuto della segnalazione;

- della relativa documentazione.

Tanto premesso, è indubbio che lo strumento più idoneo ai fini della ricezione e della successiva gestione delle segnalazioni siano le **piattaforme informatiche**. Soltanto questo strumento è infatti in grado di garantire adeguatamente la riservatezza (tramite l'utilizzo di strumenti di crittografia e, eventualmente, l'oscurazione dei dati del segnalante), la piena tracciabilità delle comunicazioni e la sicura conservazione dei dati.

Si rileva che – nonostante il Decreto consenta formalmente la trasmissione di segnalazioni, in forma scritta, anche tramite posta ordinaria e posta elettronica certificata – le Linee Guida Anac hanno da ultimo confermato le preoccupazioni, già emerse da più parti, per cui tali strumenti non sarebbero da ritenersi adeguati a garantire la riservatezza dei soggetti indicati dal Decreto e del contenuto della segnalazione.

Invero, la scelta di non adottare una piattaforma informatica e di prediligere, invece, canali di comunicazione tradizionali potrebbe comportare a carico dell'ente e del medesimo *whistleblower* oneri di non poco conto, proprio al fine di bilanciare le esigenze di riservatezza richieste dalla normativa.

La medesima ANAC, infatti, suggerisce – qualora si consenta l'invio della segnalazione tramite posta ordinaria – l'adozione di un sistema di cautele artificioso (si prevede perfino la predisposizione di tre diverse buste da parte del segnalante). Un simile sistema correrebbe il rischio di aggravare la procedura di trasmissione della segnalazione, sino a

produrre il denegato risultato di scoraggiarne l'invio.

Appare quindi opportuno – se non, addirittura, necessario – che anche le registrazioni, le trascrizioni o i verbali delle segnalazioni orali siano conservati e trattati per mezzo della piattaforma informatica (laddove presente).

In linea generale, la modalità di acquisizione per via orale delle segnalazioni deve essere, ad un tempo, prevista e scoraggiata. A titolo esemplificativo, la *policy* potrebbe prevedere che la richiesta di incontro diretto da parte del segnalante sia motivata e che la comunicazione orale non abbia una durata superiore ad un certo periodo di tempo (come, d'altro canto, disposto da ANAC con riferimento alle segnalazioni esterne).

V. A CHI È AFFIDATA LA GESTIONE DELLE SEGNALAZIONI?

Altrettanta cura è richiesta all'ente nell'attività di individuazione del soggetto deputato alla gestione delle segnalazioni.

Il Decreto chiarisce che il soggetto debba, in ogni caso, essere autonomo (*rectius* – come chiarito da ANAC – **imparziale e indipendente**).

Fermo restando tale requisito, quanto agli enti di diritto privato, la scelta è rimessa alla libera autonomia organizzativa delle società, le quali – in base al proprio assetto organizzativo e alla luce di una accurata analisi costi-benefici – sono chiamate a valutare:

- se affidare la gestione ad un soggetto interno o esterno all'ente;
- se affidare la gestione ad un organo monocratico o collegiale;

- se affidare la gestione a funzioni già attive all'interno dell'azienda o ad organo appositamente individuato.

Secondo ANAC, la scelta potrebbe ricadere su uno dei seguenti organi: **Organismo di Vigilanza** (di seguito anche "OdV"), **internal audit** e/o **comitati etici**.

Quanto agli enti pubblici, il Decreto stabilisce che nei casi in cui sia fatto obbligo di prevedere la figura del Responsabile della Prevenzione, della Corruzione e della Trasparenza ("RPCT"), le funzioni di Gestore delle segnalazioni sono affidate a quest'ultimo.

In ogni caso, il Gestore deve:

- ricevere apposita **formazione professionale** in relazione alla disciplina *whistleblowing* e in materia di *privacy*;
- essere **autorizzato al trattamento dei dati** da parte dell'Amministrazione o dell'ente titolare del trattamento (nel caso in cui il Gestore sia esterno, sarà necessaria la stipula di apposito accordo).

VI. L'OdV PUÒ ESSERE GESTORE DELLE SEGNALAZIONI?

A tale quesito si deve, in linea di principio, dare risposta affermativa.

Invero, il Decreto non prevede espressamente – come fa per il settore pubblico con la figura del RPCT – che l'OdV debba essere destinatario del flusso delle segnalazioni e gestore delle medesime. Nondimeno, dalla lettura delle disposizioni che individuano il

gestore, si deve dedurre che tale opzione non è tantomeno esclusa.

Anzi, come sopra accennato, le Linee Guida ANAC avallano esplicitamente tale possibilità.

Tanto premesso – nonostante il *placet* di ANAC – si deve rilevare che l'opzione (pur essendo la più agevole per le numerose realtà aziendali che avevano già adottato tale soluzione nell'ambito del Modello 231) lascia aperti alcuni quesiti.

In particolar modo, negli enti con numero di dipendenti superiore a 50, l'OdV – lungi dall'essere destinatario esclusivamente di segnalazioni rilevanti ai fini del Modello 231, come avvenuto sino ad oggi – sarebbe destinatario altresì della inedita tipologia di "segnalazione allargata" avente ad oggetto violazioni degli atti normativi italiani e degli atti dell'Unione Europea individuati dal Decreto.

In tal senso, ci si deve chiedere se l'Organismo sia il soggetto effettivamente idoneo a ricevere e a gestire questo tipo di segnalazioni. Diversamente, la questione non si pone con riferimento agli enti che abbiano adottato un Modello 231 e occupino meno di 50 dipendenti, in relazione ai quali il Decreto prevede che le segnalazioni possano avere ad oggetto esclusivamente reati presupposto e violazioni del Modello 231.

Negli enti di grandi dimensioni (soprattutto, nel caso in cui non vi sia un'*internal audit*) come suggerito da autorevole dottrina, il ruolo dell'OdV potrebbe preferibilmente essere quello di svolgere funzioni di vigilanza sull'adeguatezza delle procedure

whistleblowing (quali componenti del Modello 231), sul loro funzionamento, sulle attività di informazione e di formazione, nonché sugli esiti delle indagini e sui trattamenti riservati ai *whistleblowers*.

Ovviamente, tale attività presupporrebbe un flusso informativo costante da parte del gestore delle segnalazioni e non precluderebbe, ove debba ritenersi necessario, la scelta dell'Organismo di svolgere ulteriori approfondimenti e valutazioni indipendenti anche mediante l'utilizzo del proprio budget.

VII. È OPPORTUNO OPTARE PER UN CANALE INTERNO CONDIVISO?

L'art. 4 del Decreto prevede altresì la possibilità che taluni soggetti condividano il canale di segnalazione interna e la relativa gestione.

In modo particolare, per quanto concerne il settore pubblico, tale facoltà è concessa ai Comuni diversi dai capoluoghi di Provincia. Secondo ANAC, nondimeno, si deve ritenere che anche le pubbliche amministrazioni e gli enti pubblici di piccole dimensioni possano condividere la gestione del canale.

Quanto invece al settore privato, sono gli **enti di piccole dimensioni** (che abbiano impiegato, nell'ultimo anno, una media di lavoratori subordinati non superiore a 249) a poter condividere canale interno e gestore.

Con particolare riferimento alle PMI, si tratta di una scelta indubbiamente produttiva di significativi benefici in termini di semplificazione degli oneri, contenimento di costi e di specializzazione delle funzioni.

D'altro canto, è auspicabile che un simile sistema non venga adottato tra enti tra loro del tutto slegati, al fine di evitare di ingenerare confusione nei potenziali *whistleblowers*.

È noto, peraltro, che nell'ambito di gruppi di imprese fosse già frequente l'adozione di sistemi di *whistleblowing* centralizzati, eventualmente gestiti da comitati internazionali. Sul punto, la Commissione Europea ha sottolineato come al fine di garantire l'efficienza e la prossimità dei canali di segnalazione, debba essere consentito al *whistleblower* di scegliere il canale a cui rivolgersi (centrale o locale). In tal senso, i gruppi di imprese dovrebbero valutare con attenzione se rinunciare alla procedura centralizzata o prevedere un doppio canale interno (l'uno a livello della società controllata e l'altro a livello della capogruppo), lasciando al segnalante la scelta di quale canale attivare.

Ad ogni modo, come Anac non ha mancato di precisare, è necessario che il canale istituito garantisca che ciascun ente acceda esclusivamente alle segnalazioni di propria competenza, anche in considerazione della attribuzione della relativa responsabilità.

VIII. COSA DEVE FARE IL GESTORE A SEGUITO DELLA RICEZIONE DI UNA SEGNALEZIONE?

Alla luce di quanto disposto dall'art. 5 del Decreto e di quanto precisato dalle Linee Guida ANAC, le incombenze richieste per una efficace gestione della segnalazione possono essere cadenziate come di seguito:

1. entro 7 giorni, inoltrare al segnalante di un **avviso di ricevimento** della segnalazione (tale adempimento potrebbe essere facoltativo);

2. valutazione della **ammissibilità** della segnalazione;
3. qualora la segnalazione sia ammissibile, inizio dell'attività **istruttoria**;
4. entro 3 mesi dalla trasmissione dell'avviso di ricevimento (o, in mancanza dell'avviso, entro 3 mesi dalla scadenza del termine di 7 giorni dal ricevimento della segnalazione) inoltre di una comunicazione di un **riscontro** al segnalante.

Più nel dettaglio, le Linee Guida chiariscono che al Gestore compete lo svolgimento di una valutazione preliminare di ammissibilità della segnalazione.

A mero titolo esemplificativo, la segnalazione è da ritenersi **inammissibile** per i seguenti motivi:

- manifesta infondatezza per l'assenza di elementi di fatto idonei a giustificare accertamenti;
- accertato contenuto generico della segnalazione;
- segnalazione corredata da documentazione non appropriata o inconferente;
- produzione di sola documentazione in assenza della segnalazione di condotte illecite;
- sussistenza di violazioni di lieve entità.

Come anticipato, qualora il gestore ritenga ammissibile la segnalazione ricevuta, questi dà seguito alla stessa tramite lo svolgimento di attività istruttoria. Ancora a titolo esemplificativo, l'attività istruttoria può comportare interlocuzioni con il *whistleblower* (preferibilmente tramite la

piattaforma informatica), la richiesta di documenti, il coinvolgimento di altri uffici/funzioni e l'audizione di terze persone.

Il riscontro fornito al *whistleblower* all'esito dell'attività istruttoria può consistere:

- nella comunicazione della **archiviazione** con adeguata motivazione, nel caso in cui siano emersi elementi di manifesta infondatezza della segnalazione;
- nella comunicazione dell'**avvio di un'inchiesta interna**, con eventuale indicazione delle relative **risultanze**;
- nella comunicazione dei **provvedimenti** eventualmente adottati;
- nella comunicazione del **rinvio ad un'autorità competente** per ulteriori indagini.

In sostanza, dunque, salvo che il gestore non ritenga di archiviare la segnalazione, lo *step* successivo – come chiarito da ANAC – è quello dell'immediata interlocuzione con gli organi preposti interni all'ente e/o con l'istituzione o autorità esterna, ognuno secondo le proprie competenze.

Tale ultima precisazione apre a considerazioni in merito al ruolo e alle responsabilità del gestore.

Sul punto, le Linee Guida forniscono indicazioni che meritano di essere riportate testualmente: ***“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".

Con riferimento al termine di 3 mesi, indicato dal Decreto, le Linee Guida precisano infatti che il riscontro fornito entro tale scadenza possa essere di carattere **interlocutorio**. In tal caso, si renderà necessaria una ulteriore comunicazione con la quale il Gestore informa il *whistleblower* del seguito dato alla segnalazione e degli esiti dell'attività svolta.

Al di fuori dell'attività successiva alla ricezione della segnalazione, è fondamentale che il gestore si occupi di fornire informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare segnalazioni interne ed esterne.

IX. QUALI SONO GLI ADEMPIMENTI PRIVACY CUI GLI ENTI DEVONO PROVVEDERE?

Numerosi sono, infine, gli adempimenti cui – in conformità al Regolamento UE 2016/679 (GDPR) e al Codice in materia di protezione dei dati personali – ciascun ente deve provvedere nell'ambito della ricezione e gestione delle segnalazioni *whistleblowing*.

Tra questi rientrano:

- la designazione del gestore, se interno, a "**Persona Autorizzata**" al trattamento dei dati personali nell'ambito della gestione delle segnalazioni;
- la nomina del gestore, se esterno, a "**Responsabile del trattamento**" dei dati personali nell'ambito della gestione delle segnalazioni;

- la nomina del fornitore della piattaforma informatica (se presente) a "**Responsabile del trattamento**" dei dati personali in esecuzione dei servizi concordati;
- in caso di condivisione di risorse per il ricevimento e la gestione delle segnalazioni, la stipulazione di un **accordo** che regoli le rispettive responsabilità;
- la consegna di una **informativa** ai segnalanti e agli altri soggetti coinvolti nel processo di gestione della segnalazione;
- lo svolgimento di una valutazione d'impatto (**DPIA**);
- l'aggiornamento del **registro dei trattamenti**.

I. TO WHICH SUBJECTS DOES THE NEW DISCIPLINE APPLY AND FROM WHEN?

Among others, the Decree certainly has the merit of having clearly defined the subjective scope of application of the new discipline.

In addition to public sector entities, the recipients of the Whistleblowing legislation are:

- entities that have employed an average of **at least fifty employees** (with fixed-term or open-ended contracts) in the last year;
- institutions operating in **specific sectors** (banking, credit, investment, insurance and reinsurance, occupational pensions or individual pension products, securities, investment funds, payment services) even if the average number of employees is less than fifty in the last year;
- entities that have adopted **Organisational and Management Models** pursuant to Legislative Decree **No. 231/2001** (hereinafter referred to as “*231 Models*”), even if they have an average of less than fifty workers in the last year.

For the purpose of calculating the average number of employees per year, each institution must refer - from time to time - to the calendar year preceding the current one, except in the case of newly established enterprises, for which the current year is taken into account.

Again with reference to the private sector, the transitional provisions chronologically mark out the effectiveness of the provisions of the Decree, making it clear that they take effect:

- **from 15 July 2023**, for entities that have employed an average of at least 250 employees (with permanent or fixed-term employment contracts) in the last year;
- **from 17 December 2023**, for entities that employed an average of less than 250 employees in the last year.

II. WHAT CAN BE REPORTED IN ENTITIES EMPLOYING LESS THAN 50 EMPLOYEES?

In the context of entities employing fewer than 50 employees and which have adopted Models 231, reports may be made of conduct constituting offences relevant under Legislative Decree 231/2001 or violations of the Model. Such reports may be made exclusively through the internal channel set up by the entity.

On the other hand, entities employing fewer than 50 employees but operating in one of the sectors listed in the Decree - as identified above - may also report breaches of EU provisions through all reporting channels.

Of course, this possibility also applies to entities with more than 50 employees.

III. WHAT MUST THE ENTITIES DO BY THE AFOREMENTIONED DEADLINES?

The fulfilments that the entities identified above must - promptly - provide can be summarised in the following road map:

1. identification of the reporting manager (internal or external, monocratic or collegiate);
2. identification of the internal reporting channel;
3. adoption of a whistleblowing policy;
4. update of the 231 Model, the Code of Ethics and any internal documentation mentioning reporting channels;
5. privacy obligations;
6. information to persons inside and outside the organisation;
7. training of employees and manager, if internal.

First, each entity must adopt a **policy** that fully regulates whistleblowing within the same organisation.

This activity should be entrusted to a lawyer or - at any rate - to a qualified person with specific competence in the matter, possibly external to the entity.

In particular, the *policy* must:

- define the role and tasks of the persons in charge of handling alerts;
- identify the modalities and terms of data retention;
- provide for and regulate different modes of reporting (written and oral);
- provide for procedures guaranteeing the confidentiality of the whistleblower, the other persons referred to in the Decree and the content of the report;
- provide for staff awareness-raising and training initiatives to disseminate the purpose of *whistleblowing* and the procedure for its use.

At the same time, private sector entities that have adopted Models 231 will have to **update their Models**: the Decree has in fact stipulated that the latter must regulate internal reporting channels, the prohibition of retaliation and the disciplinary system. Alternatively, 231 Model will have to contain an explicit reference to the *policy*.

IV. INTERNAL CHANNEL: WHICH REPORTING MODALITIES SHOULD THE POLICY PROVIDE FOR?

The Decree requires each entity to provide, as an alternative, for two different ways of obtaining reports: in writing ("*including by computerised means*") and in oral form ("*by means of telephone lines or oral messaging systems or, at the request of the reporting person, by means of a face-to-face meeting set within a reasonable period of time*").

The only - and unavoidable - requirement is that the channels guarantee confidentiality, "*including through the use of encryption tools*":

- of the reporter;
- of the facilitator;
- of the person involved or the person otherwise mentioned in the report;
- of the content of the alert;
- of the relevant documentation.

Having said this, there is no doubt that the most appropriate tool for the receipt and subsequent handling of reports are **IT platforms**. Only this tool is in fact able to adequately guarantee confidentiality (through the use of encryption tools and, possibly, the hiding of the reporter's data), the full traceability of communications and the secure storage of data.

It should be noted that - despite the fact that the Decree formally allows the transmission of reports, in written form, also by ordinary mail and certified electronic mail - the ANAC Guidelines have recently confirmed the concerns, which had already emerged from several areas, that such instruments would not be considered adequate to guarantee the confidentiality of the persons indicated by the Decree and of the content of the report.

Indeed, the choice of not adopting an IT platform and preferring, instead, traditional channels of communication could entail considerable burdens for both the institution and the *whistleblower* himself/herself, precisely in order to balance the confidentiality requirements required by the legislation.

The same ANAC, in fact, suggests - if the sending of the report by ordinary mail is allowed - the adoption of an artificial system of precautions (it even provides for the preparation of three different envelopes by the reporter). Such a system would run the risk of aggravating the reporting procedure, to the point of producing the unfortunate result of discouraging its sending.

It therefore seems appropriate - if not, indeed, necessary - that recordings, transcripts or minutes of oral reports should also be stored and processed by means of the IT platform (where present).

As a general rule, the oral acquisition of reports should be both expected and discouraged. By way of example, the *policy* could provide that the request for a face-to-face meeting by the whistleblower should be justified and that the oral communication should not last longer than a certain period of

time (as, on the other hand, provided for by ANAC with reference to external reports).

V. TO WHOM IS THE HANDLING OF ALERTS ENTRUSTED?

Equal care is required of the institution in identifying the person in charge of handling the reports.

The Decree clarifies that the subject must, in any case, be autonomous (*rectius* - as clarified by ANAC - **impartial** and **independent**).

Notwithstanding this requirement, as far as private law entities are concerned, the choice is left up to the free organisational autonomy of the companies, which - on the basis of their organisational structure and in the light of a thorough cost-benefit analysis - are called upon to assess:

- whether to entrust management to an entity inside or outside the entity;
- whether to entrust management to a monocratic or collegiate body;
- whether to entrust the management to functions already active within the company or to a specially identified body.

According to ANAC, the choice could fall on one of the following bodies: **Supervisory Board** (hereinafter "*SB*"), **internal audit** and/or **ethics committees**.

As regards public bodies, the Decree stipulates that in cases where it is mandatory to provide for the figure of the Prevention, Corruption and Transparency Officer ("*RPCT*"), the functions of Reporting Manager are entrusted to the latter.

In any event, the Manager must:

- receive appropriate **professional training** in relation to *whistleblowing* and *privacy* regulations;
- be **authorised to process the data** by the administration or body in charge of the processing (in the event that the Manager is external, an agreement will be required).

VI. CAN THE SUPERVISORY BODY BE A REPORTING MANAGER?

This question must, in principle, be answered in the affirmative.

In fact, the Decree does not expressly provide - as it does for the public sector with the figure of the *RPCT* - that the Supervisory Board must be the recipient of the flow of reports and the manager of such reports. Nevertheless, from reading the provisions identifying the manager, it must be inferred that this option is not ruled out.

Indeed, as mentioned above, the ANAC Guidelines explicitly endorse this possibility.

Having said this - despite ANAC's approval - it must be noted that this option (despite being the easiest for the many companies that had already adopted this solution within the 231 Model) leaves some questions open.

In particular, in entities with more than 50 employees, the Supervisory Board - far from being the exclusive recipient of reports relevant for the purposes of the 231 Model, as has been the case to date - would also be the recipient of the unprecedented type of 'extended report' concerning violations of Italian legislative acts and European Union acts identified by the Decree.

In this sense, the question arises as to whether the SB is actually the appropriate entity to receive and handle this type of report. On the contrary, the question does not arise with regard to entities that have adopted a 231 Model and employ fewer than 50 employees, in relation to which the Decree provides that reports may relate exclusively to predicate offences and violations of the 231 Model.

In large entities (especially where there is no internal audit), as suggested by authoritative doctrine, the role of the SB might preferably be to perform supervisory functions on the adequacy of whistleblowing procedures (as components of the 231 Model), their functioning, information and training activities, as well as on the outcomes of investigations and the treatment of whistleblowers.

Obviously, such an activity would presuppose a constant flow of information from the reporting manager and would not preclude, where deemed necessary, the choice of the SB to carry out further in-depth investigations and independent assessments also through the use of its own budget.

VII. IS IT APPROPRIATE TO OPT FOR A SHARED INTERNAL CHANNEL?

Article 4 of the Decree also provides for the possibility of certain institutions sharing the internal reporting channel and its management.

In particular, as far as the public sector is concerned, this option is granted to municipalities other than provincial capitals. According to ANAC, however, it must be

assumed that public administrations and small public bodies can also share the management of the channel.

As for the private sector, it is the **small entities** (employing an average of no more than 249 employees in the last year) that can share the internal channel and manager.

With particular reference to small and medium entities, this choice is undoubtedly productive of significant benefits in terms of simplification of burdens, cost containment and specialisation of functions.

On the other hand, it is desirable that such a system should not be adopted between entities that are completely unrelated to each other, in order to avoid confusing potential whistleblowers.

It is known, moreover, that within groups of companies the adoption of centralised *whistleblowing* systems, possibly managed by international committees, was already common. On this point, the European Commission emphasised that in order to ensure the efficiency and proximity of the whistleblowing channels, the whistleblower should be allowed to choose the channel to which he/she wishes to turn (central or local). In this sense, groups of companies should carefully consider whether to forego the centralised procedure or to provide for a dual internal channel (one at the level of the subsidiary and the other at the level of the parent company), leaving the whistleblower the choice of which channel to activate.

In any case, as ANAC has not failed to point out, it is necessary that the channel set-up

ensures that each institution only accesses reports falling within its competence, also in view of the allocation of the relevant responsibility.

VIII. WHAT SHOULD THE MANAGER DO FOLLOWING RECEIPT OF A REPORT?

In the light of the provisions of Article 5 of the Decree and the ANAC Guidelines, the tasks required for the effective management of the report can be broken down as follows:

1. within 7 days, forward an **acknowledgement of receipt** of the report to the reporter (this would appear to be optional);
2. assessment of the **admissibility** of the alert;
3. if the report is admissible, commencement of the **internal investigation**;
4. within 3 months of the transmission of the acknowledgement of receipt (or, in the absence of an acknowledgement, within 3 months of the expiry of the 7-day time limit from receipt of the report) forwarding a **feedback** to the reporter.

More specifically, the Guidelines clarify that the Manager is responsible for carrying out a preliminary assessment of the admissibility of the report.

By way of example only, the report is **inadmissible** for the following reasons:

- manifestly unfounded due to the absence of factual elements capable of justifying findings;
- ascertained generic content of the report;

- report accompanied by inappropriate or irrelevant documentation;
- production of only documentation in the absence of a report of unlawful conduct;
- existence of minor infringements.

As mentioned above, if the manager deems the report received to be admissible, he follows it up by carrying out investigative activities. Again by way of example, the investigative activity may involve interlocations with the whistleblower (preferably through the IT platform), requests for documents, the involvement of other offices/departments and speaking with third persons.

The feedback provided to the whistleblower at the outcome of the investigation activity may consist of:

- the communication of the **filing** with adequate **justification**, if elements of manifest unfoundedness of the report have come to light;
- the announcement of the **opening of an internal investigation**, possibly including the **findings**;
- the communication of any **measures** taken;
- the notification of the **referral to a competent authority** for further investigation.

In essence, therefore, unless the manager decides to file the report, the next step - as clarified by ANAC - is that of immediate interlocation with the bodies in charge within the institution and/or with the external institution or authority, each according to its competences.

This last clarification opens up considerations regarding the role and responsibilities of the manager.

On this point, the Guidelines provide indications that deserve to be quoted verbatim: ***'It is not for the person in charge of handling the report to ascertain individual responsibilities, whatever their nature, nor to carry out legitimacy or substantive checks on the acts and measures adopted by the reporting body/administration, under penalty of encroaching on the competences of the persons in charge of such matters within each body or administration or of the judiciary'***.

With reference to the time limit of three months, indicated by the Decree, the Guidelines specify that the feedback provided within this deadline may be of an **interlocutory** nature. In such a case, a further communication will be required in which the Manager informs the whistleblower of the action taken on the report and the outcome of the activity performed.

Outside the activity following the receipt of the report, it is crucial that the manager takes care to provide clear information on the channel, procedures and prerequisites for internal and external reporting.

IX. WHAT ARE THE PRIVACY REQUIREMENTS TO BE FULFILLED BY ENTITIES?

Finally, there are numerous obligations to which - in accordance with EU Regulation 2016/679 (GDPR) and the Personal Data Protection Code - each institution must comply when receiving and handling whistleblowing reports.

These include:

- the designation of the manager, if internal, as an **“Authorised Person”** for the processing of personal data in the context of alert management;
- the appointment of the manager, if external, as **“Data Processor”** of personal data in the context of the handling of alerts;
- the appointment of the IT platform provider (if any) as **“Data Processor”** of personal data in performance of the agreed services;
- in the case of shared resources for receiving and handling alerts, the conclusion of an **agreement** regulating the respective responsibilities;
- the delivery of a **report** to the whistleblowers and other persons involved in the process of handling the report;
- carrying out an **impact assessment**;
- the updating of the **data processing register**.

CONTATTI



Giuseppe Fornari

Founding Partner

g.fornari@fornarieassociati.com



Enrico Di Fiorino

Partner

e.difiorino@fornarieassociati.com



Pasquale Grella

Of Counsel

p.grella@fornarieassociati.com



Martina Pangallo

Associate

m.pangallo@fornarieassociati.com

Milano

Via Chiossetto 18

T: +39 0254122206

E: milano@fornarieassociati.com

Roma

Piazza Adriana 5

T: +39 0622201000

E: roma@fornarieassociati.com

Bari

Via Principe Amedeo 25

T: +39 080 918 4280

E: bari@fornarieassociati.com

Questa pubblicazione ha lo scopo di fornire informazioni di carattere generale rispetto all'argomento trattato e non deve quindi essere considerata come un parere legale né come una disamina esaustiva di ogni aspetto relativo alla materia oggetto del documento.

This publication is intended to provide general information with respect to the subject matter and should therefore not be regarded as legal advice nor as an exhaustive examination of every aspect of the subject matter.

Fornari e Associati
www.fornarieassociati.com