Live Webinar

Il Whistleblowing: tra Legislazione Italiana, Direttiva UE 2019/1937 e Norma ISO 37002:2021

Relatori

Ing. Ciro Alessio STRAZZERI

Dott. Gianluca INCANI

27 Maggio 2021

DIGITALPA
Software & Servizi per PA e Aziende

GRUPPOSTRAZZERI
KNOWLEDGE SHARING

Asso 231
STAKEHOLDERS A CONFRONTO

GIACC ITALY
Global Infrastructure Anti-Corruption Centre

Anti Bribery ACADEMY

Ing. Ciro Alessio Strazzeri

Presidente Asso231

Unica associazione multistakeholders del settore, studia e risolve problematiche connesse all'applicazione del Decreto 231/2001.

D. Lgs. 231/2001

Esperto 231, Auditor 231,
Componente OdV certificato (KHC)

Auditor certificato

Auditor ISO 37001 certificate (KHC)
Auditor ISO 45001 certificate (KHC)

Presidente GIACC Italy

Affiliata a Global Infrastructure Anti- Corruption Centre con sede in UK, aumenta la consapevolezza della corruzione e promuove l'attuazione di misure *anti-corruzione* come parte integrante delle attività delle organizzazioni pubbliche e private.

CEO Gruppo Strazzeri Franchising

Multinazionale eroga attività di Risk&Compliance Management, Auditing e Training oltre che di consulenza per l'internazionalizzazione delle organizzazioni pubbliche e private. .

Dott. Gianluca Incani

Consultant ***Trasparenza Amministrativa e Anticorruzione****,*
Giornalista specializzato in ICT della Pubblica Amministrazione,
ha collaborato con Norme & Tributi del Sole 24 Ore, già Editor presso Maggioli Editore.
Ha alle spalle oltre **1000 ore di formazione e consulenza** per i più importanti Enti Territoriali, Camere di Commercio e Società Pubbliche nazionali. Autore di webinar professionali per PA, collaborazione con il progetto ***Città Digitali della Fondazione Censis.***

Il Whistleblowing: origine del termine

Con il termine "whistleblowing" si indica l'istituto di origine anglosassone, dall'inglese "to blow the whistle" – "soffiare il fischietto", in riferimento alla denuncia o segnalazione da parte di un individuo di attività illecite o fraudolente all'interno un'organizzazione pubblica, privata, o di un 'azienda.

All'origine del termine ***«whistleblower»*** ci dovrebbe essere il bobbies inglese che soffia nel proprio fischietto per destare attenzione e mettere in fuga i malintenzionati.

Tradotto letteralmente, il whistleblower è il soffiatore nel fischietto, ovvero colui il quale "segnala" a qualcuno i comportamenti illeciti di qualcun altro.

Il ***«whistleblowing»***, quindi, è un sistema di segnalazioni di violazioni, da parte del dipendente o di un terzo interessato di un'organizzazione pubblica o privata, che ha il coraggio di denunciare atti corruttivi o irregolarità di cui sia venuto a conoscenza, utilizzando canali anonimi, sicuri e indipendenti per mantenere segreta la propria identità, mettendosi a riparo da eventuali ritorsioni e discriminazioni, conseguenti la segnalazione.

Il whistleblowing nella Pubblica Amministrazione

- **D.lg. 165/2001, art. 54-bis (Tutela del dipendente pubblico che segnala illeciti)**, inserito dalla legge 190/2012, per come modificato dall'art. 1 della **Legge 30 novembre 2017, n. 179 «Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato».**

I

1. **Il pubblico dipendente** che, nell'interesse dell'integrità della pubblica amministrazione, segnala al responsabile della prevenzione della corruzione e della trasparenza, ovvero all'ANAC, o denuncia all'autorità giudiziaria ordinaria o a quella contabile, **condotte illecite** di cui è venuto a conoscenza in ragione del proprio rapporto di lavoro non può essere sanzionato, demansionato, licenziato, trasferito, o sottoposto ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro determinata dalla segnalazione.

Il

L'adozione di misure ritenute ritorsive, di cui al primo periodo, nei confronti del segnalante è comunicata in ogni caso all'ANAC dall'interessato o dalle organizzazioni sindacali maggiormente rappresentative nell'amministrazione nella quale le stesse sono state poste in essere.

L'ANAC informa il Dipartimento della funzione pubblica della Presidenza del Consiglio dei ministri o gli altri organismi di garanzia o di disciplina per le attività e gli eventuali provvedimenti di competenza.

III

2. Ai fini del presente articolo, per dipendente pubblico si intende il dipendente delle amministrazioni pubbliche di cui all'articolo 1, comma 2, ivi compreso il dipendente di cui all'articolo 3, il dipendente di un ente pubblico economico ovvero il dipendente di un ente di diritto privato sottoposto a controllo pubblico ai sensi dell'articolo 2359 del codice civile.

La disciplina di cui al presente articolo si applica anche ai lavoratori e ai collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'amministrazione pubblica.

IV

3. L'identità del segnalante non può essere rivelata.

Nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'art. 329 c.p.p.

Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria.

Nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa.

V

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

VI

4.La segnalazione è sottratta all'accesso previsto dagli artt 22 e ss. della legge n. 241/1990.

5.L'ANAC, sentito il Garante per la protezione dei dati personali, adotta apposite **linee guida** relative alle procedure per la presentazione e la gestione delle segnalazioni. Le linee guida prevedono l'utilizzo di modalità anche informatiche e promuovono il ricorso a strumenti di crittografia per garantire la riservatezza dell'identità del segnalante e per il contenuto delle segnalazioni e della relativa documentazione.

VII

6. Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro.

Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro.

Qualora venga accertato il mancato svolgimento da parte del responsabile di attivita' di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. L'ANAC determina l'entità della sanzione tenuto conto delle dimensioni dell'amministrazione o dell'ente cui si riferisce la segnalazione.

VIII

7.E' a carico dell'amministrazione pubblica o dell'ente di cui al comma 2 dimostrare che le misure discriminatorie o ritorsive, adottate nei confronti del segnalante, sono motivate da ragioni estranee alla segnalazione stessa. Gli atti discriminatori o ritorsivi adottati dall'amministrazione o dall'ente sono nulli.

8.Il segnalante che sia licenziato a motivo della segnalazione è reintegrato nel posto di lavoro ai sensi dell'articolo 2 del decreto legislativo 4 marzo 2015, n. 23.

IX

9. Le tutele di cui al presente articolo non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione o comunque per reati commessi con la denuncia di cui al comma 1 ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave.

Linee-guida ANAC

- Regolamento per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio, in vigore dal 3 settembre 2020
- Linee-guida in materia di tutela del dipendente pubblico che segnala illeciti (**Determinazione n. 6 del 28/04/2015**)
- Si vedano anche i quattro rapporti annuali sull'applicazione del whistleblowing (22 giugno 2016; 22 giugno 2017; 28 giugno 2018; 16 luglio 2019)

Codice autodisciplina società quotate, luglio 2015

- Il Comitato ritiene che, **almeno nelle società emittenti appartenenti all'indice FTSE-MIB** (*principale indice di benchmark dei mercati azionari italiani; coglie circa l'80% della capitalizzazione di mercato interna n.d.r.*), un adeguato sistema di controllo interno e di gestione dei rischi debba essere dotato di un **sistema interno di segnalazione** da parte dei dipendenti di eventuali irregolarità o violazioni della normativa applicabile e delle procedure interne (c.d. sistemi di whistleblowing) in linea con le best practices esistenti in ambito nazionale e internazionale, che garantiscano un canale informativo specifico e riservato nonché l'anonimato del segnalante.

L'estensione al settore bancario

- **Testo Unico Bancario, art. 52-*bis* (Sistemi interni di segnalazione delle violazioni)**, inserito dal d.lg. n. 72 del 12 maggio 2015

I

- 1. **Le banche e le relative capogruppo** adottano procedure specifiche per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una **violazione delle norme disciplinanti l'attività bancaria**.

Il

2. Le procedure di cui al comma 1 sono idonee a:

a)garantire la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione;

b)tutelare adeguatamente il soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;

c)assicurare per la segnalazione un canale specifico, indipendente e autonomo.

III

3.La presentazione di una segnalazione non costituisce di per sé violazione degli obblighi derivanti dal rapporto di lavoro.

4.La disposizione di cui all'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196 (*articolo abrogato dal d.lg. 101/2018)*, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

5. La Banca d'Italia emana disposizioni attuative del presente articolo.

IV

- Art. 52-*ter* (Segnalazione di violazioni alla Banca d'Italia)

1.La Banca d'Italia riceve, da parte del personale delle banche e delle relative capogruppo, segnalazioni che si riferiscono a violazioni riguardanti norme del titolo II e III, nonché atti dell'Unione europea direttamente applicabili nelle stesse materie.

2.La Banca d'Italia tiene conto dei criteri di cui all'articolo 52-*bis* , comma 2, lettere *a)* e *b)* , e può stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni.

V

3.La Banca d'Italia si avvale delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza e per il perseguimento delle finalità previste dall'articolo 5.

4.Nel caso di accesso ai sensi degli articoli 22, e seguenti, della legge 7 agosto 1990, n. 241, l'ostensione del documento è effettuata con modalità che salvaguardino comunque la riservatezza del segnalante. Si applica l'articolo 52-*bis* , commi 3 e 4.

Le Disposizioni di vigilanza Banca d'Italia

(Circolare 21 luglio 2015)

In linea con il principio di proporzionalità, le banche definiscono i sistemi interni volti a permettere la segnalazione da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria (ex art. 10 TUB).

I sistemi interni di segnalazione garantiscono in ogni caso la riservatezza e la protezione dei dati personali del soggetto che effettua la segnalazione e del Soggetto eventualmente segnalato.

I suddetti sistemi sono strutturati in modo da garantire che le segnalazioni vengano ricevute, esaminate e valutate attraverso canali specifici, autonomi e indipendenti che differiscono dalle ordinarie linee di reporting.

Il

- A tal fine, i sistemi interni di segnalazione prevedono canali alternativi a disposizione del segnalante in modo da assicurare che il soggetto preposto alla ricezione, all'esame e alla valutazione della segnalazione non sia gerarchicamente o funzionalmente subordinato all'eventuale soggetto segnalato, non sia esso stesso il presunto responsabile della violazione e non abbia un potenziale interesse correlato alla segnalazione tale da comprometterne l'imparzialità e l'indipendenza di giudizio.

III

I soggetti preposti alla ricezione, all'esame e alla valutazione delle segnalazioni non partecipano all'adozione degli eventuali provvedimenti decisionali, che sono rimessi alle funzioni o agli organi aziendali competenti.

Le banche nominano un **responsabile dei sistemi interni di segnalazione** il quale assicura il corretto svolgimento del procedimento e riferisce direttamente e senza indugio agli organi aziendali le informazioni oggetto di segnalazione, ove rilevanti.

I soggetti che ricevono, esaminano e valutano le segnalazioni, il responsabile dei sistemi interni di segnalazione e ogni altro soggetto coinvolto nella procedura hanno l'obbligo di garantire la confidenzialità delle informazioni ricevute, anche in merito all'identità del segnalante che, in ogni caso, deve essere opportunamente tutelato da condotte ritorsive, discriminatorie o comunque sleali conseguenti alla segnalazione.

IV

I sistemi interni di segnalazione prevedono:

a.i soggetti che, in conformità a quanto disposto dall'art. 1, comma 2, lett. h-novies, TUB, li possono attivare;

b.fermo restando quanto previsto dall'art. 52-bis, comma 1, TUB, gli atti o i fatti che possono essere oggetto di segnalazione;

c.le modalità attraverso cui segnalare le presunte violazioni e i soggetti preposti alla ricezione delle segnalazioni;

V

d. il procedimento che si instaura nel momento in cui viene effettuata una segnalazione con l'indicazione, ad esempio, dei tempi e delle fasi di svolgimento del procedimento, dei soggetti coinvolti nello stesso, delle ipotesi in cui il responsabile dei sistemi interni di segnalazione è tenuto a fornire immediata comunicazione agli organi aziendali;

e. le modalità attraverso cui il soggetto segnalante e il soggetto segnalato devono essere informati sugli sviluppi del procedimento;

VI

f. l'obbligo per il soggetto segnalante di dichiarare se ha un interesse privato collegato alla segnalazione;
g. nel caso in cui il segnalante sia corresponsabile delle violazioni, un trattamento privilegiato per quest'ultimo rispetto agli altri corresponsabili, compatibilmente con la disciplina applicabile.

VII

- Al fine di incentivare l'uso dei sistemi interni di segnalazione e di favorire la diffusione di una cultura della legalità, le banche illustrano al proprio personale in maniera chiara, precisa e completa il procedimento di segnalazione interno adottato indicando i presidi posti a garanzia della riservatezza dei dati personali del segnalante e del presunto responsabile della violazione con l'espresso avvertimento che la disposizione di cui all'art. 7, comma 2, del decreto legislativo 20 giugno 2003, n. 196 (*articolo abrogato dal d.lg. 101/2018)*, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

VIII

- Nel rispetto di quanto previsto dalla disciplina sulla protezione dei dati personali, il responsabile dei sistemi interni di segnalazione redige una relazione annuale sul corretto funzionamento dei sistemi interni di segnalazione, contenente le informazioni aggregate sulle risultanze dell'attività svolta a seguito delle segnalazioni ricevute, che viene approvata dagli organi aziendali e messa a disposizione al personale della banca.

IX

- Le banche, fermo restando il rispetto delle disposizioni di cui alla presente Sezione e alle Sezioni IV e V, possono esternalizzare l'attività di ricezione, esame e valutazione delle segnalazioni.
- Il responsabile dei sistemi interni di segnalazione, in linea con il principio di proporzionalità, può direttamente gestire le fasi di ricezione, esame e valutazione del procedimento di segnalazione.

L'estensione al settore finanziario

- **Testo Unico Finanza, art. 4-*undecies* (Sistemi interni di segnalazione delle violazioni)**, in vigore dal 3 gennaio 2018.

I

- 1. **I soggetti di cui alle parti II** (*disciplina degli intermediari n.d.r.*) **e III** (*disciplina dei mercati n.d.r.*) adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire violazioni delle norme disciplinanti l'attività svolta, nonchè del regolamento UE n. 596/2014 (*Market Abuse Regulation n.d.r.*).

Il

2. Le procedure previste al comma 1 sono idonee a garantire:

a)la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione; l'identità del segnalante è sottratta all'applicazione dell'articolo 7, comma 2, del decreto legislativo 30 giugno 2003, n. 196 (*articolo abrogato dal d.lg. 101/2018)*, e non può essere rivelata per tutte le fasi della procedura, salvo suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato;

b)la tutela adeguata del soggetto segnalante contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;

c) un canale specifico, indipendente e autonomo per la segnalazione.

III

3.Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del Codice civile, la presentazione di una segnalazione nell'ambito della procedura di cui al comma 1 non costituisce violazione degli obblighi derivanti dal rapporto di lavoro.

4.La Banca d'Italia e la Consob adottano, secondo le rispettive competenze, le disposizioni attuative del presente articolo, avuto riguardo all'esigenza di coordinare le funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti destinatari.

IV

- Art. 4-*duodecies* (Procedura di segnalazione alle Autorità di Vigilanza).

1. Le Autorità di cui all'articolo 4, comma 1:

a)ricevono, ciascuna per le materie di propria competenza, da parte del personale dei soggetti indicati dall'articolo 4-*undecies*, segnalazioni che si riferiscono a violazioni delle norme del presente decreto, nonché di atti dell'Unione europea direttamente applicabili nelle stesse materie;

b)tengono conto dei criteri previsti all'articolo 4-*undecies*, comma 2, lettere a) e b), e possono stabilire condizioni, limiti e procedure per la ricezione delle segnalazioni;

V

c)si avvalgono delle informazioni contenute nelle segnalazioni, ove rilevanti, esclusivamente nell'esercizio delle funzioni di vigilanza;

d)prevedono, mediante protocollo d'intesa, le opportune misure di coordinamento nello svolgimento delle attività di rispettiva competenza, ivi compresa l'applicazione delle relative sanzioni, in modo da coordinare l'esercizio delle funzioni di vigilanza e ridurre al minimo gli oneri gravanti sui soggetti vigilati.

2. Gli atti relativi alle segnalazioni di cui al comma 1 sono sottratti all'accesso previsto dagli articoli 22 e ss. della legge n. 241/1990.

L'estensione alle Imprese Assicurative

- **Decreto legislativo 21 maggio 2018 n. 68, attuativo della Direttiva U.E. 2016/97 sulla distribuzione assicurativa**
- Inserisce nel Codice delle Assicurazioni gli artt 10-*quater* e 10-*quinquies*

art. 10-*quater* (Sistemi interni di segnalazione delle violazioni)

l. Le imprese di assicurazione o di riassicurazione, gli intermediari assicurativi e riassicurativi, inclusi gli intermediari assicurativi a titolo accessorio, adottano procedure specifiche per la segnalazione al proprio interno, da parte del personale, di atti o fatti che possano costituire **violazioni delle norme disciplinanti l'attività svolta**, di cui al presente codice.

Il

2. Le procedure previste al comma l sono idonee a garantire:

a)la riservatezza dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità amministrativa o giudiziaria in relazione ai fatti oggetto della segnalazione;

b)la protezione adeguata dei dipendenti dei soggetti di cui al comma l e, ove possibile, di altre persone che riferiscono di violazioni commesse all'interno degli stessi almeno contro ritorsioni, discriminazioni e altri tipi di trattamento iniquo;

c) un canale specifico, indipendente ed autonomo per la segnalazione.

III

3. Fuori dei casi di responsabilità a titolo di calunnia o diffamazione, ovvero per lo stesso titolo ai sensi dell'articolo 2043 del codice civile, la presentazione di una segnalazione nell'ambito della procedura di cui al comma l non costituisce violazione degli obblighi derivanti dal rapporto di lavoro.

4. La disposizione di cui all'articolo 7, comma 2, del d.lgs. n. 196/2003 (*articolo abrogato dal d.lg. 101/2018)*, non trova applicazione avuto riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso quando la conoscenza sia indispensabile per la difesa del segnalato.

Le imprese di assicurazione o di riassicurazione, gli intermediari assicurativi e riassicurativi, inclusi gli intermediari assicurativi a titolo accessorio osservano le disposizioni di attuazione del presente articolo emanate dall'IVASS.

art. 10-*quinquies* (Procedura di segnalazione di violazioni)

l. L'IVASS:

a) riceve segnalazioni da parte dei dipendenti dei soggetti di cui all'articolo 10-quater, comma 1, riguardanti violazioni delle norme del presente codice, nonché di disposizioni dell'Unione europea direttamente applicabili;

b) stabilisce condizioni, limiti e procedure per la ricezione delle segnalazioni;

c)si avvale delle informazioni contenute nelle segnalazioni, ove rilevanti esclusivamente nell'esercizio delle funzioni di vigilanza;

2. Gli atti relativi alle segnalazioni di cui al comma 1 sono sottratti all'accesso previsto dagli articoli 22 e ss. della legge n. 241/1990

L'estensione alla normativa antiriciclaggio

- **D.lg. 231/2007, art. 48 (Sistemi interni di segnalazione delle violazioni)**, come modificato dal d.lg. 90/2017, in vigore dal 4 luglio 2017.

1. **I soggetti obbligati** adottano procedure per la segnalazione al proprio interno da parte di dipendenti o di persone in posizione comparabile di **violazioni, potenziali o effettive, delle disposizioni dettate in funzione di prevenzione del riciclaggio e del finanziamento del terrorismo**.

Il

2. Le procedure di cui al comma 1 garantiscono:

a)la tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni;

b)la tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;

c)lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente, proporzionato alla natura e alle dimensioni del soggetto obbligato.

III

3.La presentazione della segnalazione di cui al presente articolo non costituisce, di per se', violazione degli obblighi derivanti dal rapporto contrattuale con il soggetto obbligato.

4.La disposizione di cui all'articolo 7, comma 2, del d.lgs. n. 196/2003 (*articolo abrogato dal d.lg. 101/2018)*, non trova applicazione con riguardo all'identità del segnalante, che può essere rivelata solo con il suo consenso o quando la conoscenza sia indispensabile per la difesa del segnalato.

L'inserimento del whistleblowing neiModelli organizzativi ex d.lg. 231/2001

- **D.lg. 231/2001, art 6, comma 2-bis,** introdotto dall'art. 2 della Legge 30 novembre 2017 n. 179, in vigore dal 29 dicembre 2017:

Il

I modelli organizzativi prevedono:

a)uno o più canali che consentano ai **soggetti indicati nell'articolo 5**, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di **condotte illecite, rilevanti ai sensi del presente decreto** e fondate su elementi di fatto precisi e concordanti, o di **violazioni del modello di organizzazione e gestione** dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;

b)almeno un canale alternativo di segnalazione idoneo a garantire, **con modalità informatiche**, la riservatezza dell'identità del segnalante;

D.Lgs. 231/01

Art. 5, comma 1

a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unita' organizzativa dotata di autonomia finanziaria e funzionale nonche' da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso;

b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

III

c)il divieto di atti di ritorsione o discriminatori, diretti o indiretti, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d)nel sistema disciplinare adottato ai sensi del comma 2, lettera e), **sanzioni nei confronti di chi viola le misure di tutela del segnalante**, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

CNDCEC(ABI, Confindustria, Consiglio Nazionale Forense), dicembre 2018

- *«Principi consolidati per la redazione dei modelli organizzativi e l'attività dell'organismo di vigilanza e prospettive di revisione del d.lgs. 8 giugno 2001, n. 231»*

…Da quanto fin qui analizzato, si può affermare quanto meno che gli enti debbano dotarsi di strumenti più avanzati della semplice casella di posta elettronica dedicata all'Organismo di Vigilanza, soprattutto ai fini della riservatezza sull'identità del segnalante, nonché definire meccanismi di verifica della fondatezza della segnalazione.

L'individuazione di una procedura *ad hoc* è necessaria anche in relazione alle attività da intraprendere nel caso di risposta alla segnalazione, definendo una specifica metodologia e individuando i soggetti coinvolti, nonché i tempi e gli strumenti di verifica da utilizzare.

IV

- Inoltre:

2-ter. L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni può essere denunciata all'Ispettorato nazionale del lavoro, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

V

2-quater. Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo.

Sono altresì nulli il mutamento di mansioni ai sensi dell'articolo 2103 del codice civile, nonchè qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.

E' onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa

VI

- Infine (art. 3 della Legge 179/2017):

Nelle ipotesi di segnalazione effettuata nelle forme e nei limiti sopra previsti, il "perseguimento dell'interesse all'integrità dell'ente nonché alla prevenzione e alla repressione delle malversazioni" costituisce **giusta causa di rivelazione** di notizie coperte dall'obbligo di segreto professionale (art 622 c.p.) e scientifico/industriale (art 623 c.p.) e rientranti nell'obbligo di fedeltà del lavoratore ex art 2105 c.c.

Quanto appena detto non vale nel caso in cui l'obbligo di segreto professionale gravi su chi sia venuto a conoscenza della notizia **in ragione di un rapporto di consulenza professionale** o di assistenza con l'ente, l'impresa o la persona fisica interessata.

VII

Quando notizie e documenti che sono comunicati all'organo deputato a riceverli siano oggetto di segreto aziendale o professionale, costituisce violazione del relativo obbligo di segreto la rivelazione con modalità eccedenti rispetto alle finalità dell'eliminazione dell'illecito e, in articolare, la rivelazione al di fuori del canale di comunicazione specificamente predisposto a tal fine.

VIII

- La legge n. 179 non prevede il limite al diritto di accesso da parte del segnalato prima sancito dall'art 7 del Codice Privacy (oggi abrogato).
- Tuttavia il d.lg. 101/2018 ribadisce il limite a tale diritto se dal suo esercizio può derivare in concreto un danno «alla riservatezza dell'identità del dipendente che segnala, ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio».
- Si noti che il riferimento riguarda esclusivamente la segnalazione ai sensi della legge n. 179 (cioè nell'ambito del Modello 231 e dei dipendenti pubblici) e non anche quella effettuata ai sensi del TUF, del TUB, della legge antiriciclaggio e del Codice Assicurazioni.

Direttiva 2019/1937

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

- Protezione delle persone che segnalano violazioni del diritto UE
- In corso di recepimento [LEGGE 22 aprile 2021, n. 53 Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea - Legge di delegazione europea 2019-2020. (21G00063) (GU Serie Generale n.97 del 23-04-2021) Entrata in vigore del provvedimento: 08/05/2021]

Direttiva 2019/1937 - Definizioni

Vedi Art. 5 della Direttiva

Non si usano i termini «Whistleblowing»/»Whistleblower» nelle definizioni.

Note: nei vari «Considerando» si usa spesso – «Act as whistleblowers»

Direttiva 2019/1937 - Finalità

La direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, entrata in vigore il 16 dicembre 2019, reca disposizioni volte a fornire ai segnalanti (o whistleblowers) una tutela uniforme in tutti gli Stati membri e armonizzata tra i vari settori, introducendo regole comuni che impongano l'adozione di canali di segnalazione efficaci, riservati e sicuri e, al tempo stesso, garantiscano una protezione efficace degli informatori da possibili ritorsioni.

Direttiva 2019/1937 – Ambito di applicazione

Il Capo I (artt. 1-6) contiene le disposizioni relative all'ambito di applicazione, alle definizioni e alle condizioni di protezione. In particolare l'ambito di applicazione oggettivo è esteso (art. 2) a tutti i casi in cui vengano segnalate violazioni del diritto dell'Unione, definite come atti od omissioni illecite ovvero che vanificano l'oggetto e le finalità di norme dell'Unione relative agli specifici settori individuati nell'allegato alla Direttiva, relativi a settori quali gli appalti pubblici, la prevenzione del riciclaggio e del finanziamento del terrorismo, la sicurezza dei prodotti, la tutela dell'ambiente e la salute pubblica etc…

Direttiva 2019/1937 – Whistleblowers

Per quanto attiene all'ambito di applicazione soggettivo il whistleblower è definito come la persona fisica che segnala o divulga informazioni sulle violazioni acquisite nell'ambito delle sue attività professionali, a prescindere dalla natura di tali attività o del fatto che il rapporto di lavoro sia nel frattempo terminano o non ancora iniziato.

Direttiva 2019/1937 – Soggetti segnalanti

Nello specifico, rientrano tra i segnalanti tutelati dalla Direttiva le persone aventi la qualifica di "lavoratori" ai sensi dell'art. 45 TFUE, ossia le persone che nel settore privato come in quello pubblico forniscono, per un certo periodo di tempo, a favore di terzi e sotto la direzione di questi, determinate prestazioni verso il corrispettivo di una retribuzione.
La protezione deve, quindi, essere concessa anche ai lavoratori con contratti atipici, quali quello a tempo parziale e a tempo determinato, nonché a chi ha un contratto o un rapporto di lavoro con un'agenzia interinale, ai tirocinanti e ai volontari. Le medesime tutele devono, altresì, essere applicate a lavoratori autonomi, consulenti, subappaltatori e fornitori (esposti a ritorsioni quali la risoluzione o l'annullamento del contratto di servizi, della licenza o del permesso, il boicottaggio o l'inserimento in liste nere). Sono, infine, tutelati gli azionisti e le persone negli organi direttivi (che potrebbero subire ritorsioni in termini finanziari o danni alla reputazione).

Direttiva 2019/1937 – Soggetti terzi

Inoltre, la Direttiva (art. 4) impegna gli Stati ad estendere le misure di protezione non soltanto ai segnalanti che lavorano nel settore privato o pubblico, bensì anche ai c.d. facilitatori, ossia coloro che assistono "una persona segnalante nel processo di segnalazione in un contesto lavorativo e la cui assistenza deve essere riservata" (art. 5), ai terzi connessi con le persone segnalanti, quali ad esempio colleghi o familiari, e ai soggetti giuridici collegati al segnalante (ritorsioni indirette potrebbero essere quelle intraprese contro il soggetto giuridico di cui il segnalante sia proprietario, per cui lavori o a cui sia altrimenti connesso, quali l'annullamento della fornitura di servizi o il boicottaggio).

Direttiva 2019/1937 – Segnalazioni anonime

Fatti salvi gli obblighi vigenti di prevedere la segnalazione anonima in forza del diritto dell'Unione, la presente direttiva non pregiudica la facoltà degli Stati membri di decidere se i soggetti giuridici del settore pubblico o del settore privato e le autorità competenti debbano accettare le segnalazioni anonime di violazioni e darvi seguito.

Le persone che hanno segnalato o divulgato pubblicamente informazioni su violazioni in forma anonima, ma che successivamente sono state identificate e hanno subito ritorsioni, possono nondimeno beneficiare della protezione prevista ai sensi del capo VI, a condizione che soddisfino le condizioni di cui al paragrafo 1 dell'art. 6.

Direttiva 2019/1937 – Requisiti per tutela

Le tutele previste dalla Direttiva sono concesse nel caso in cui siano segnalate violazioni già commesse o non ancora commesse (ma che molto verosimilmente potrebbero esserlo), atti od omissioni che il segnalante abbia fondati motivi di ritenere violazioni, nonché tentativi di nascondere violazioni. Sono, tuttavia, stabiliti alcuni specifici requisiti per poter accedere alle tutele. Innanzitutto, il segnalante deve avere ragionevoli motivi, alla luce delle circostanze e delle informazioni di cui dispone al momento della segnalazione, per ritenere che i fatti che segnala siano veri. Inoltre, è necessario che il segnalante abbia fondati motivi per ritenere che le informazioni segnalate rientrino nell'ambito di applicazione della Direttiva stessa (art. 6). Tale requisito garantisce che chi fornisce deliberatamente informazioni errate o fuorvianti sia escluso dalla protezione e che, al contrario, possa beneficiare delle tutele chi effettua una segnalazione imprecisa in buona fede. Si pone, quindi, come una garanzia essenziale contro le segnalazioni dolose, futili o infondate. È necessario che il segnalante abbia fondati motivi per ritenere che le informazioni segnalate rientrino nell'ambito di applicazione della Direttiva stessa.

Direttiva 2019/1937 – Canali di segnalazione

La proposta inziale presentata dalla Commissione Europea prevedeva che per poter godere delle tutele previste dalla Direttiva, i segnalanti dovevano, in primo luogo, utilizzare i canali interni; se questi non funzionavano o non avevano possibilità di successo, dovevano rivolgersi alle autorità esterne e, solo come ultima possibilità, potevano rendere le informazioni di dominio pubblico.

In fase di approvazione, il meccanismo, tuttavia, è stato modificato e ai whistleblowers è ora riconosciuta la facoltà di scegliere il canale che ritengono più appropriato, anche se la divulgazione al pubblico è ancora soggetta ad alcune condizioni.

Direttiva 2019/1937 – Segnalazioni interne

Il Capo II (artt. 7-9), contiene le disposizioni relative alle segnalazioni interne e al seguito delle stesse. In particolare si chiede agli Stati di "incoraggiare la segnalazione mediante canali di segnalazione interni prima di effettuare la segnalazione mediante canali di segnalazione esterni" (art. 7). Tale regola, subisce alcune eccezioni, specificamente indicate:

-nel caso in cui non si ritenga che la segnalazione possa essere gestita efficacemente a 'livello interno' e sussiste un rischio di ritorsione;

-nel caso in cui è ammissibile una segnalazione diretta ai media in deroga ai canali whistleblowing.

Direttiva 2019/1937 – Soggetti obbligati

La Direttiva (art. 8) impone l'obbligo di istituire canali di segnalazione interni a tutte le imprese con almeno 50 lavoratori, indipendentemente dalla natura delle loro attività, nonché a tutti i soggetti giuridici del settore pubblico, compresi quelli di proprietà o sotto il controllo degli stessi. L'esenzione delle piccole e medie imprese da tale obbligo non si applica, tuttavia, ai soggetti che operano nel settore dei servizi finanziari esposti a rischio di riciclaggio e finanziamento del terrorismo che, pertanto, dovranno istituire canali di segnalazione interni indipendentemente dalle loro dimensioni. Inoltre, a seguito di un'opportuna valutazione del rischio, è riconosciuta agli Stati membri la facoltà di esigere che anche società con un numero di dipendenti inferiore istituiscano canali di segnalazione interna in casi specifici, per esempio a causa dei notevoli rischi che possono derivare dalle loro attività. Nel settore pubblico, invece, l'obbligo di istituire canali whistleblowing potrà essere derogato - a discrezione del singolo Stato membro - per i soli Comuni con meno di 10.000 abitanti.

Direttiva 2019/1937 – Procedure di segnalazione

Quanto alle procedure per la segnalazione interna, sono imposti (art. 9) una serie di requisiti che gli enti devono rispettare, riconoscendo, al tempo stesso, che spetti comunque a ciascun soggetto definire il tipo di canale da istituire. Nello specifico i canali per ricevere le segnalazioni devono essere progettati, realizzati e gestiti in modo sicuro e tale da garantire la riservatezza dell'identità del segnalante, nonché di eventuali terzi citati nella segnalazione. Al whistleblower deve essere consentito di segnalare per iscritto e di trasmettere le segnalazioni per posta, mediante cassetta per i reclami o piattaforma online o di segnalare oralmente mediante linea telefonica gratuita o altro sistema di messaggistica vocale, o entrambi. Inoltre, su richiesta del segnalante, deve essere possibile effettuare segnalazioni mediante incontri di persona con i soggetti incaricati.

Direttiva 2019/1937 – Tempi di gestione

Sono altresì imposte determinate tempistiche: entro sette giorni il segnalante deve ricevere un avviso circa il ricevimento della segnalazione stessa e le procedure

devono prevedere un termine ragionevole (non superiore a tre mesi) per dare un riscontro alla segnalazione.

Direttiva 2019/1937 – Soggetti gestori

I canali di segnalazione possono essere gestiti internamente da una persona o da un servizio designato a tal fine o essere messi a disposizione esternamente da terzi, purché offrano adeguate garanzie di indipendenza, riservatezza, protezione dei dati e segretezza. È, inoltre, necessario che sia designata una persona o un servizio imparziale competente per dare seguito alle segnalazioni, che potrebbe essere la stessa persona o lo stesso servizio che riceve le segnalazioni e che manterrà la comunicazione con il segnalante. Un seguito diligente, se previsto dal diritto nazionale, dovrà essere garantito anche per le segnalazioni anonime.

Direttiva 2019/1937 – Segnalazioni esterne

Il Capo III (artt. 10-14) disciplina le segnalazioni esterne e il relativo seguito. Quanto alle segnalazioni esterne, i whistleblowers possono segnalare violazioni alle autorità designate dagli Stati membri, nonché a quelle competenti a livello europeo. Sono quindi disciplinati: l'obbligo di istituire canali di segnalazione esterna e di seguito alle segnalazioni, i criteri per la progettazione dei canali di segnalazione esterna (affinché gli stessi vengano considerati indipendenti e autonomi); le informazioni sul ricevimento delle segnalazioni e relativo seguito che le autorità competenti devono pubblicare sui loro siti web, in una sezione separata, facilmente identificabile e accessibile.

Direttiva 2019/1937 – Divulgazioni pubbliche

Il Capo IV (art. 15) riconosce la possibilità di effettuare divulgazioni pubbliche in alcuni specifici casi. In particolare, in tali circostanze, i segnalanti beneficiano delle protezioni previste a condizione che:

- abbiano prima segnalato internamente ed esternamente o direttamente esternamente, ma non sia stata intrapresa un'azione appropriata in risposta alla segnalazione entro il termine di tre mesi previsto dalla direttiva oppure
- la persona segnalante aveva fondati motivi di ritenere che:

i)la violazione possa costituire un pericolo imminente o palese per il pubblico interesse, come nel caso in cui sussista una situazione di emergenza o il rischio di danno irreversibile; oppure

ii)in caso di segnalazione esterna, sussista il rischio di ritorsioni o le prospettive che la violazione sia affrontata efficacemente siano scarse per via delle circostanze del caso di specie, come quelle in cui possano essere occultate o distrutte prove oppure in cui un'autorità possa essere collusa con l'autore della violazione o coinvolta nella violazione stessa.

Direttiva 2019/1937 – Riservatezza

Il Capo V (artt. 16-18) contiene disposizioni concernenti:

•l'obbligo di riservatezza, specificando l'obbligo per gli Stati membri di provvedere affinché l'identità della persona segnalante non sia divulgata, senza il suo consenso esplicito, a nessuno che non faccia parte del personale autorizzato competente a ricevere o a dare seguito alle segnalazioni. Sono inoltre previsti specifici casi di deroga e le relative garanzie;

- il trattamento dei dati personali;
- la conservazione della documentazione inerente alle segnalazioni; tutti i dati e

le informazioni relativi alla segnalazione devono essere conservati diligentemente in modo da poterle fornire alle autorità competenti se necessario.

Direttiva 2019/1937 – Documentazione telefonate

Se per la segnalazione si utilizza una linea telefonica o un altro sistema di messaggistica vocale strato, subordinatamente al consenso della persona segnalante, i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti hanno il diritto di documentare la segnalazione orale:

a) facendo una registrazione della conversazione (per le linee registrate) su un supporto durevole che consenta l'accesso alle informazioni; o

b) mediante una trascrizione completa e accurata della conversazione effettuata dal personale addetto al trattamento della segnalazione.

I soggetti giuridici del settore privato e del settore pubblico e le autorità competenti consentono alla persona segnalante di verificare, rettificare e approvare la trascrizione della chiamata mediante l'apposizione della propria firma.

Direttiva 2019/1937 – Documentazione incontri

Se una persona chiede un incontro con il personale dei soggetti giuridici del settore privato e del settore pubblico o delle autorità competenti ai fini di una segnalazione ai sensi dell'articolo 9, paragrafo 2, e dell'articolo 12, paragrafo 2, i soggetti giuridici del settore privato e del settore pubblico e le autorità competenti assicurano, subordinatamente al consenso della persona segnalante, che sia conservata una documentazione completa e accurata di tale incontro su un supporto durevole che consenta l'accesso alle informazioni.

I soggetti giuridici del settore privato e del settore pubblico e le autorità competenti hanno il diritto di documentare l'incontro:

a) facendo una registrazione della conversazione su un supporto durevole che consenta l'accesso alle informazioni; o

b)mediante un verbale dettagliato dell'incontro redatto dal personale addetto al trattamento della segnalazione.

I soggetti giuridici del settore privato e pubblico e le autorità competenti offrono alla persona segnalante la possibilità di verificare, rettificare e approvare il verbale dell'incontro mediante l'apposizione della propria firma.

Direttiva 2019/1937 – Misure di protezione

Il Capo VI (artt.19-24) concerne le misure di protezione. In particolare gli Stati membri dovranno adottare le misure necessarie per:

- vietare qualsiasi forma di ritorsione;

•garantire che siano fornite informazioni pertinenti e accurate a tale riguardo in modo chiaro e facilmente accessibile al pubblico;

•assicurare consulenze individuali, imparziali e riservate a titolo gratuito, nonché –sempre che ricorrano determinate condizioni - il patrocinio gratuito nei procedimenti penali;

•prevedere che una volta che il whistleblower abbia dimostrato di aver effettuato una segnalazione a norma della Direttiva e di aver subito un danno, l'onere della prova sia spostato sulla persona che ha compiuto l'azione ritorsiva;

•garantire l'impossibilità nei confronti del segnalante di far valere obblighi giuridici o contrattuali come le clausole di lealtà dei contratti o gli accordi di riservatezza o non divulgazione per impedire di effettuare una segnalazione, negare la protezione o penalizzare le persone segnalanti per aver effettuato la segnalazione,

•escludere, nei procedimenti giudiziari, la responsabilità del segnalante per effetto di segnalazioni o divulgazioni pubbliche;

•escludere la responsabilità dei segnalanti per l'acquisizione delle informazioni segnalate o divulgate pubblicamente né per l'accesso alle stesse, purché tale acquisizione o accesso non costituisca di per sé un reato.

Direttiva 2019/1937 – Divieto di ritorsione

Il timore di ritorsioni è il principale ostacolo alla diffusione della cultura della segnalazione delle violazioni. La Direttiva vieta qualsiasi forma di ritorsione, diretta o indiretta, attuata, incoraggiata o tollerata da parte dei datori di lavoro, dei clienti, dei destinatari dei servizi e delle persone che lavorano per l'organizzazione o per conto di quest'ultima, compresi i colleghi del segnalante e i dirigenti della stessa organizzazione o di altre organizzazioni con le quali il segnalante sia in contatto nell'ambito della sua attività professionale. Nel recepire il nuovo testo di legge, pertanto, gli Stati membri dovranno adottare le misure necessarie per vietare qualsiasi forma di ritorsione, comprese le minacce e i tentativi di ritorsione quale, per esempio, il licenziamento, la retrocessione o la mancata promozione, l'imposizione di misure disciplinari, la discriminazione, l'inserimento in liste nere, la conclusione anticipata di contratti per beni o servizi, l'annullamento di licenze o permessi, i danni, anche alla reputazione della persona, in particolare sui social media o la sottoposizione ad accertamenti psichiatrici o medici.

Direttiva 2019/1937 – Sanzioni

A tutela del sistema di protezione dei segnalanti previsto dalla Direttiva, gli Stati membri sono chiamati a prevedere sanzioni – di natura civile, penale o amministrativa – effettive, proporzionate e dissuasive nei confronti:

- di coloro che ostacolano o tentano di ostacolare le segnalazioni; attuano atti di ritorsione o procedimenti vessatori contro i segnalanti; violano l'obbligo di riservatezza sull'identità delle persone segnalanti.
- delle persone segnalanti per le quali sia accertato che hanno scientemente effettuato segnalazioni o divulgazioni pubbliche false.

Inoltre gli Stati membri provvedono affinché i diritti e i mezzi di ricorso previsti dalla presente direttiva non possano essere oggetto di rinuncia o limitazione in virtù di accordi, regimi, forme o condizioni di lavoro, compreso un accordo arbitrale precontenzioso.

Direttiva 2019/1937 – Disposizioni finali

Il Capo VII contiene le disposizioni finali.

In particolare, il termine di recepimento della Direttiva è fissato al 17 dicembre 2021; per quanto riguarda i soggetti giuridici del settore privato con più di 50 e meno di 250 lavoratori, gli Stati membri mettono in vigore le disposizioni legislative, regolamentari e amministrative necessarie per conformarsi all'obbligo di stabilire un canale di segnalazione interno entro il 17 dicembre 2023 (articolo 26).

L'articolo 25 ha per oggetto il trattamento più favorevole e la clausola di non regressione. Prevede infatti che gli Stati membri possano introdurre o mantenere disposizioni più favorevoli ai diritti delle persone segnalanti di quelle previste dalla presente direttiva, e che l'attuazione di questa non possa in alcun caso costituire motivo di riduzione del livello di protezione già offerto dagli Stati membri nei settori cui si applichi la direttiva.

Confronto tra L. 179/17 e Direttiva 2019/1937

- La normativa italiana si applica, nel settore privato, solo agli enti che hanno adottato un Modello organizzativo ex d.lg. 231/2001.
- La Direttiva riguarda tutte le imprese con almeno 50 dipendenti, a prescindere dall'adozione del Modello organizzativo, nonché ai soggetti operanti nei servizi finanziari e a rischio riciclaggio/finanziamento del terrorismo, indipendentemente dalle dimensioni. Gli Stati membri possono decidere di applicare la Direttiva anche a soggetti con meno di 50 dipendenti.

Il

- La legge 179 tutela il segnalante nei casi di condotte illecite rilevanti ai fini dei reati presupposto ex d.lg. 231/2001 e violazioni del Modello organizzativo.
- La Direttiva considera tutte le violazioni relative ad alcuni specifici settori del diritto dell'Unione, tra i quali rientrano appalti, servizi finanziari, sicurezza dei prodotti e dei trasporti, tutela dell'ambiente e dei consumatori.

III

- Quanto alla categoria dei segnalanti, la legge 179 tutela i destinatari del Modello organizzativo, quindi dipendenti, amministratori e terze parti.
- La Direttiva tutela gli azionisti delle società, i dipendenti, i soggetti che assistono i whistleblower, gli ex dipendenti e coloro che hanno conosciuto gli illeciti in fase di selezione o negoziazione precontrattuale.

IV

- La legge 179 richiede agli enti di adottare uno o più canali (dei quali ameno uno in forma informatica) che consentano le segnalazioni garantendo la riservatezza dell'identità del segnalante.
- Secondo la Direttiva, gli enti dovranno:

a) individuare un soggetto – interno o esterno – per la gestione e l'analisi delle segnalazioni nonché un soggetto che si occupi di seguire le indagini e mantenere la comunicazione con il segnalante

b)consentire al whistleblower di effettuare segnalazioni scritte, orali (incluso via telefono e messaggio vocale) o di persona

c) comunicare la ricezione della segnalazione entro 7 giorni;

d)prendere in carico le segnalazioni e mantenere il whistleblower informato entro un tempo ragionevole (non oltre 3 mesi)

e) conservare traccia e archiviare le segnalazioni e i relativi follow up

f) fornire informazioni chiare e dettagliate sulle procedure di segnalazione interna.

V

- La legge 179 sancisce il divieto di atti di ritorsione o discriminatori nei confronti del whistleblower, per motivi collegati, direttamente o indirettamente, alla segnalazione. Inoltre, sono nulli il licenziamento ritorsivo o discriminatorio del segnalante, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei suoi confronti.
- Secondo la Direttiva, è vietata qualsiasi forma di ritorsione, comprese le minacce e i tentativi di ritorsione quale, per esempio, il licenziamento, l'imposizione di misure disciplinari, l'inserimento in liste nere, l'annullamento di licenze o permessi, i danni, anche alla reputazione della persona, in particolare sui social media o la sottoposizione ad accertamenti psichiatrici o medici.
- Sono, altresì, vietate le ritorsioni indirette che possono essere intraprese contro il soggetto giuridico di cui il segnalante sia proprietario, per cui lavori o a cui sia altrimenti connesso in un contesto lavorativo.

ISO 37001:2016 – Segnalazione di sospetti

8.9 Segnalazione di sospetti

L'organizzazione deve attuare procedure che:

a) favoriscano e consentano alle persone di segnalare in buona fede o sulla base di una ragionevole convinzione atti di corruzione tentati, presunti ed effettivi, oppure qualsiasi violazione o carenza concernente il sistema di gestione per la prevenzione della corruzione alla funzione di conformità per la prevenzione della corruzione o al personale preposto (sia direttamente che mediante un parte terza appropriata);

b) ad eccezione di un procedimento richiesto per procedere ad un'indagine, prevedano che l'organizzazione tratti le segnalazioni in via confidenziale, in modo da proteggere l'identità di chi segnala e di altri coinvolti o menzionati nella segnalazione;

c) consentano la segnalazione in forma anonima;

d) vietino ritorsioni e proteggano coloro che effettuano le segnalazioni dalle ritorsioni, dopo avere in buona fede, o sulla base di una convinzione ragionevole, sollevato o riferito sospetti circa atti di corruzione tentati, certi o presunti oppure violazioni concernenti la politica per la prevenzione della corruzione o il sistema di gestione per la prevenzione della corruzione;

e) permettano al personale di ricevere consulenze da una persona appropriata su cosa fare quando ci si trova dinanzi a un sospetto o a una situazione che possa comprendere atti di corruzione.

L'organizzazione deve garantire che tutti i membri del personale siano edotti sulle procedure di segnalazione e siano in grado di utilizzarle, e che siano consapevoli dei loro diritti e delle loro tutele in base a tali procedure.

Nota 1 Tali procedure possono essere le medesime o fare parte di quelle utilizzate per segnalare altri casi sospetti (per esempio sicurezza, negligenza, illeciti o altri rischi gravi).

Nota 2 L'organizzazione può servirsi di un socio in affari per gestire il sistema per suo conto.

Nota 3 In alcune giurisdizioni, i requisiti di cui sopra ai punti b) e c) sono vietati per legge. In tali casi, l'organizzazione documenta la propria impossibilità a conformarsi.

ISO 37001:2016 – Indagini e gestione della corruzione

8.10 Indagini e gestione della corruzione

L'organizzazione deve attuare procedure che:

a) richiedano la valutazione, e se necessario, l'indagine di qualsiasi atto di corruzione o violazione della politica di prevenzione della corruzione o al sistema di gestione per la prevenzione della corruzione, che sia riferito, rilevato o ragionevolmente presunto;

b) richiedano azioni appropriate nel caso in cui l'indagine riveli qualsivoglia atto di corruzione o violazione della politica di prevenzione della corruzione o al sistema di gestione per la prevenzione della corruzione;

c) diano potere e capacità d'azione agli investigatori;

d) richiedano la collaborazione nell'ambito dell'indagine da parte del personale pertinente;

e) richiedano che lo stato e i risultati dell'indagine siano riferiti alla funzione di conformità per la prevenzione della corruzione e alle altre funzioni di conformità, nel modo opportuno;

f) richiedano che l'indagine sia svolta in maniera riservata e che i risultati di tale indagine siano riservati.

L'indagine deve essere condotta da parte di, e riferita a, membri del personale che non facciano parte del ruolo o della funzione oggetto di indagine. L'organizzazione può nominare un socio in affari affinché svolga l'indagine e comunichi i risultati a membri del personale che non facciano parte del ruolo o della funzione oggetto di indagine.

Nota 1 Vedere punto A.18 per una guida.

Nota 2 In alcune giurisdizioni, il requisito di cui sopra al punto f) è vietato per legge. In tal caso, l'organizzazione documenta la propria impossibilità a conformarsi.

ISO 37301:2021 – Raising concerns

8.3 Raising concerns

The organization shall establish, implement and maintain a process to encourage and enable the reporting of (in cases of reasonable grounds to believe that the information is true) attempted, suspected or actual violations of the compliance policy or compliance obligations.

This process shall:

— be visible and accessible throughout the organization;

— treat reports confidentially;

— accept anonymous reports;

— protect those making reports from retaliation;

— enable personnel to receive advice.

The organization shall ensure that all personnel are aware of the reporting procedures, their rights and protections and are able to use them.

ISO 37301:2021 – Investigation processes

8.4 Investigation processes

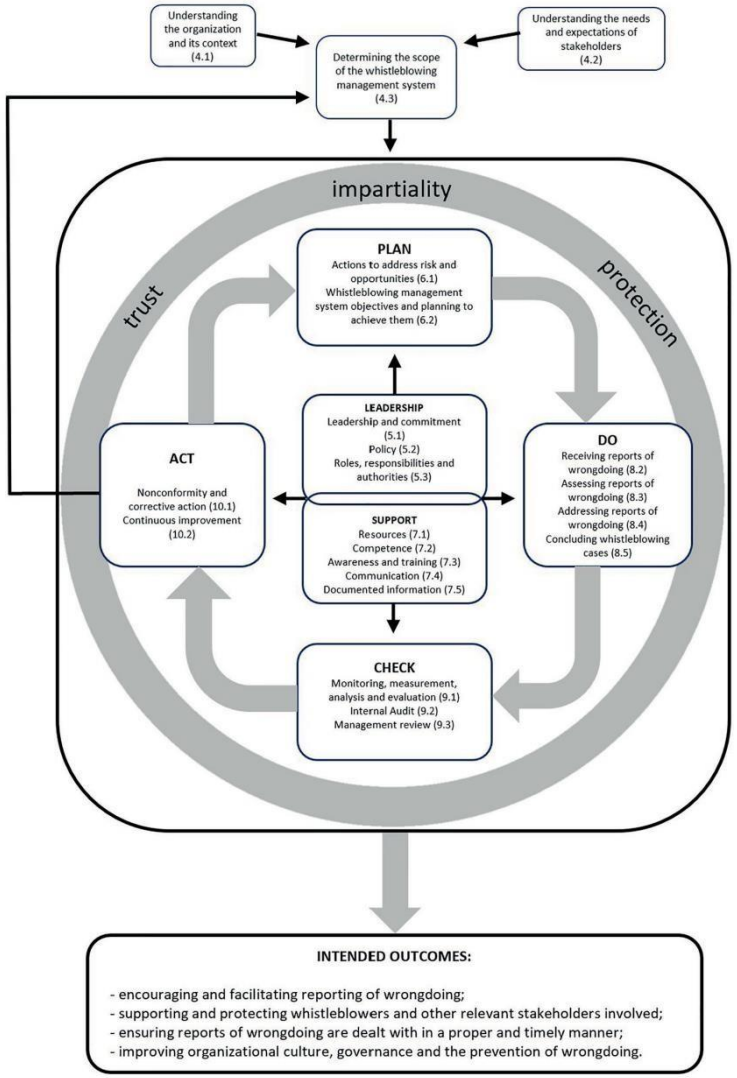
The organization shall develop, establish, implement and maintain processes to assess, evaluate, investigate and close reports on suspected or actual instances of noncompliance. These processes shall ensure fair and impartial decision-making.

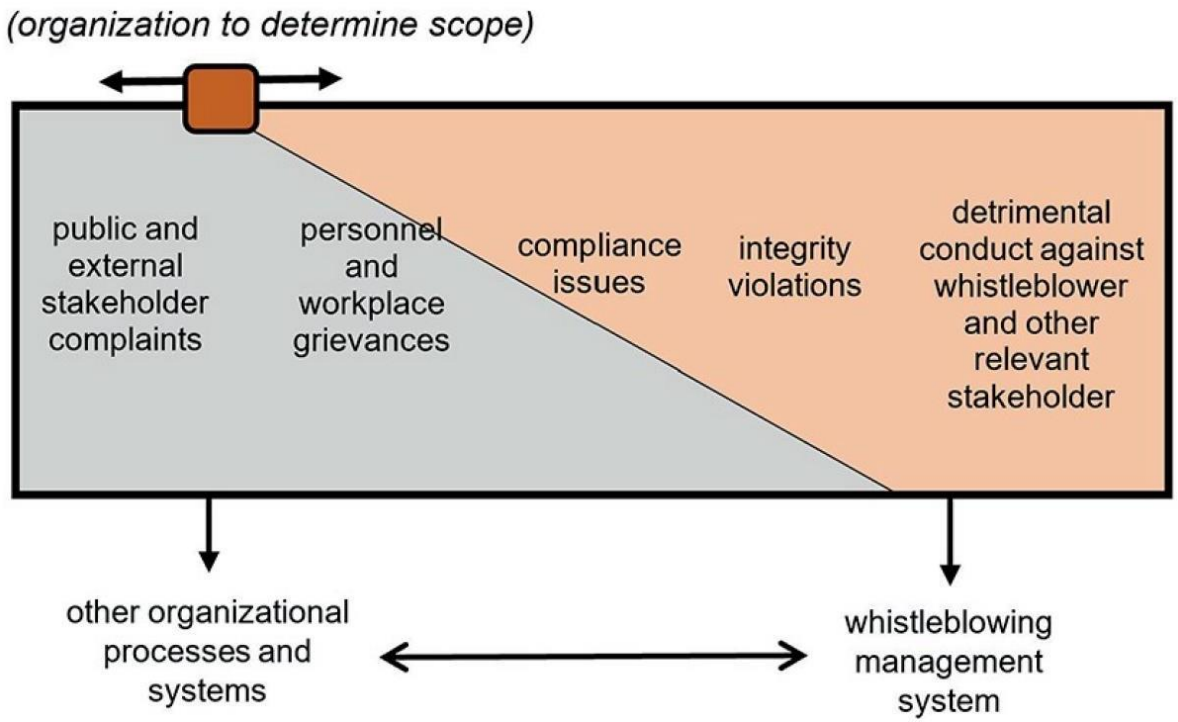
The investigation processes shall be carried out independently and without conflict of interests by competent personnel.

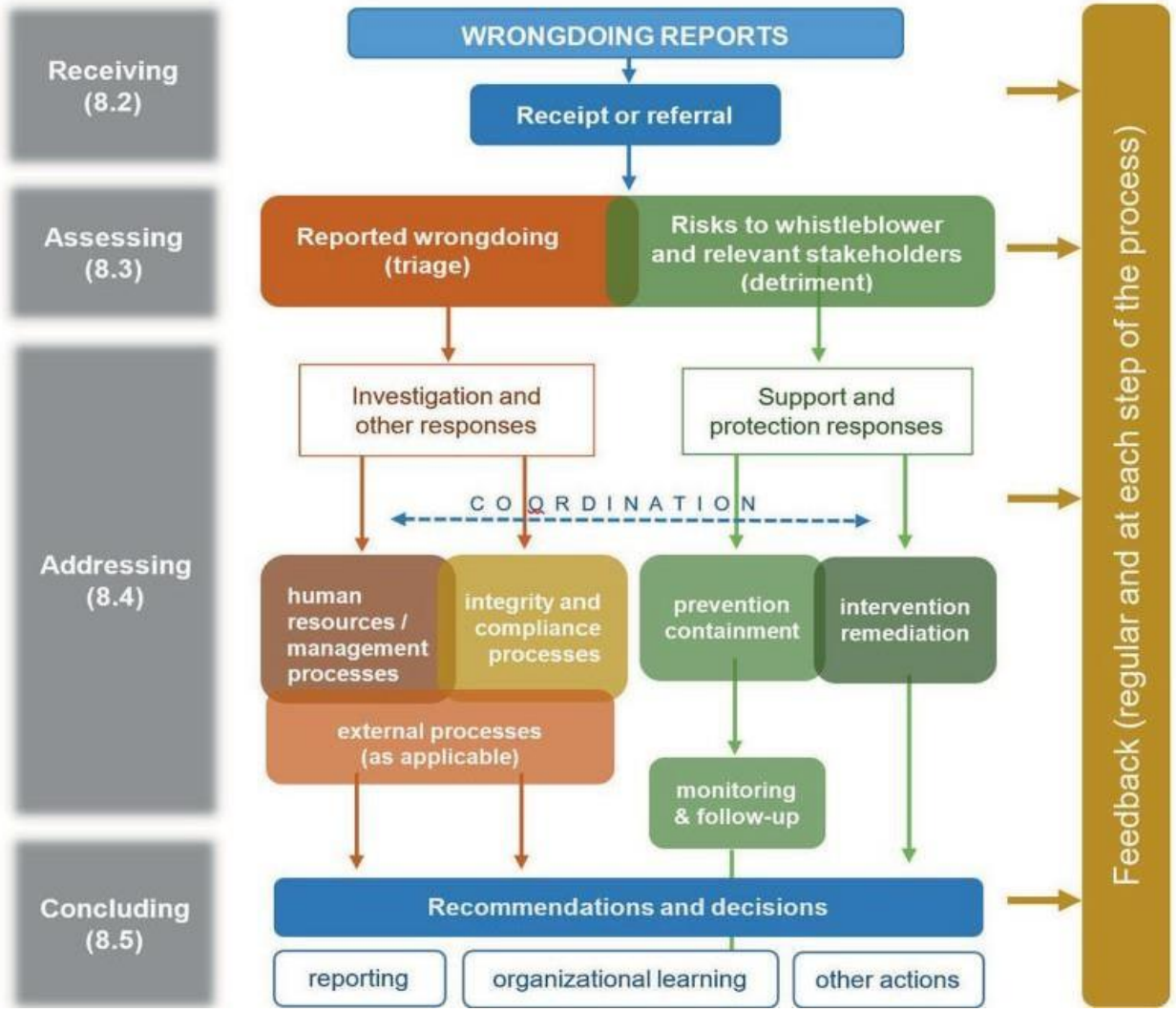
The organization shall use the outcomes of investigations for the improvement of the compliance management system as appropriate (see Clause 10).

The organization shall regularly report on the numbers and outcomes of investigations to the governing body or top management.

The organization shall retain documented information on the investigation.


Understanding the organization and its context (4.1)
Understanding the needs and expectations of stakeholders (4.2)
Determining the scope of the whistleblowing management system (4.3)
impartiality
trust
protection
PLAN
Actions to address risk and opportunities (6.1)
Whistleblowing management system objectives and planning to achieve them (6.2)
LEADERSHIP
Leadership and commitment (5.1)
Policy (5.2)
Roles, responsibilities and authorities (5.3)
ACT
Nonconformity and corrective action (10.1)
Continuous improvement (10.2)
DO
Receiving reports of wrongdoing (8.2)
Assessing reports of wrongdoing (8.3)
Addressing reports of wrongdoing (8.4)
Concluding whistleblowing cases (8.5)
SUPPORT
Resources (7.1)
Competence (7.2)
Awareness and training (7.3)
Communication (7.4)
Documented information (7.5)
CHECK
Monitoring, measurement, analysis and evaluation (9.1)
Internal Audit (9.2)
Management review (9.3)
INTENDED OUTCOMES:
- encouraging and facilitating reporting of wrongdoing;
- supporting and protecting whistleblowers and other relevant stakeholders involved;
- ensuring reports of wrongdoing are dealt with in a proper and timely manner;
- improving organizational culture, governance and the prevention of wrongdoing.


(organization to determine scope)
public and external stakeholder complaints
personnel and workplace grievances
compliance issues
integrity violations
detrimental conduct against whistleblower and other relevant stakeholder
other organizational processes and systems
whistleblowing management system


Receiving (8.2)
Assessing (8.3)
Addressing (8.4)
Concluding (8.5)
WRONGDOING REPORTS
Receipt or referral
Reported wrongdoing (triage)
Risks to whistleblower and relevant stakeholders (detriment)
Investigation and other responses
Support and protection responses
COORDINATION
human resources / management processes
integrity and compliance processes
prevention containment
intervention remediation
external processes (as applicable)
monitoring & follow-up
Recommendations and decisions
reporting
organizational learning
other actions
Feedback (regular and at each step of the process)

Ulteriore documentazione utile

- *La disciplina del whistleblowing: indicazioni e spunti operativi per i professionisti*, CNDCEC, 12 febbraio 2021
- *La disciplina in materia di whistleblowing*, Confindustria, 2018
- *A Best Practice Guide for Whistleblowing Legislation*, Transparency international, 2018
- *Linee guida per la predisposizione di procedure in materia di whistleblowing*, Transparency Italia, 2016

Grazie per l'attenzione!

CioAlessioStrazzeri

Mobile:3388395177–Email:info@gruppostrazzeri.it

I NOSTRI COMPAGNI DI VIAGGIO

Responsabilità e Sanzioni

Responsabilità - Amministrazioni Pubbliche

«**Dlgs 165/2001 art. 54bis comma 6**. Qualora venga accertata, nell'ambito dell'istruttoria condotta dall'ANAC, l'adozione di misure discriminatorie da parte di una delle amministrazioni pubbliche o di uno degli enti di cui al comma 2, fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile che ha adottato tale misura una sanzione amministrativa pecuniaria da 5.000 a 30.000 euro.

Qualora venga accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi a quelle di cui al comma 5, l'ANAC applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro. Qualora venga accertato il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute, si applica al responsabile la sanzione amministrativa pecuniaria da 10.000 a 50.000 euro.»

I NOSTRI COMPAGNI DI VIAGGIO

Responsabilità e Sanzioni

ARTICOLO 54-bis comma 6 del decreto legislativo n. 165/2001

1

sanzione amministrativa pecuniaria

Da € 5.000 a € 30.000

Verso il responsabile di adozione di misure discriminatorie

2

sanzione amministrativa pecuniaria

Da € 10.000 a € 50.000

Se accertata l'assenza di procedure per l'inoltro e la gestione delle segnalazioni ovvero l'adozione di procedure non conformi

3

sanzione amministrativa pecuniaria

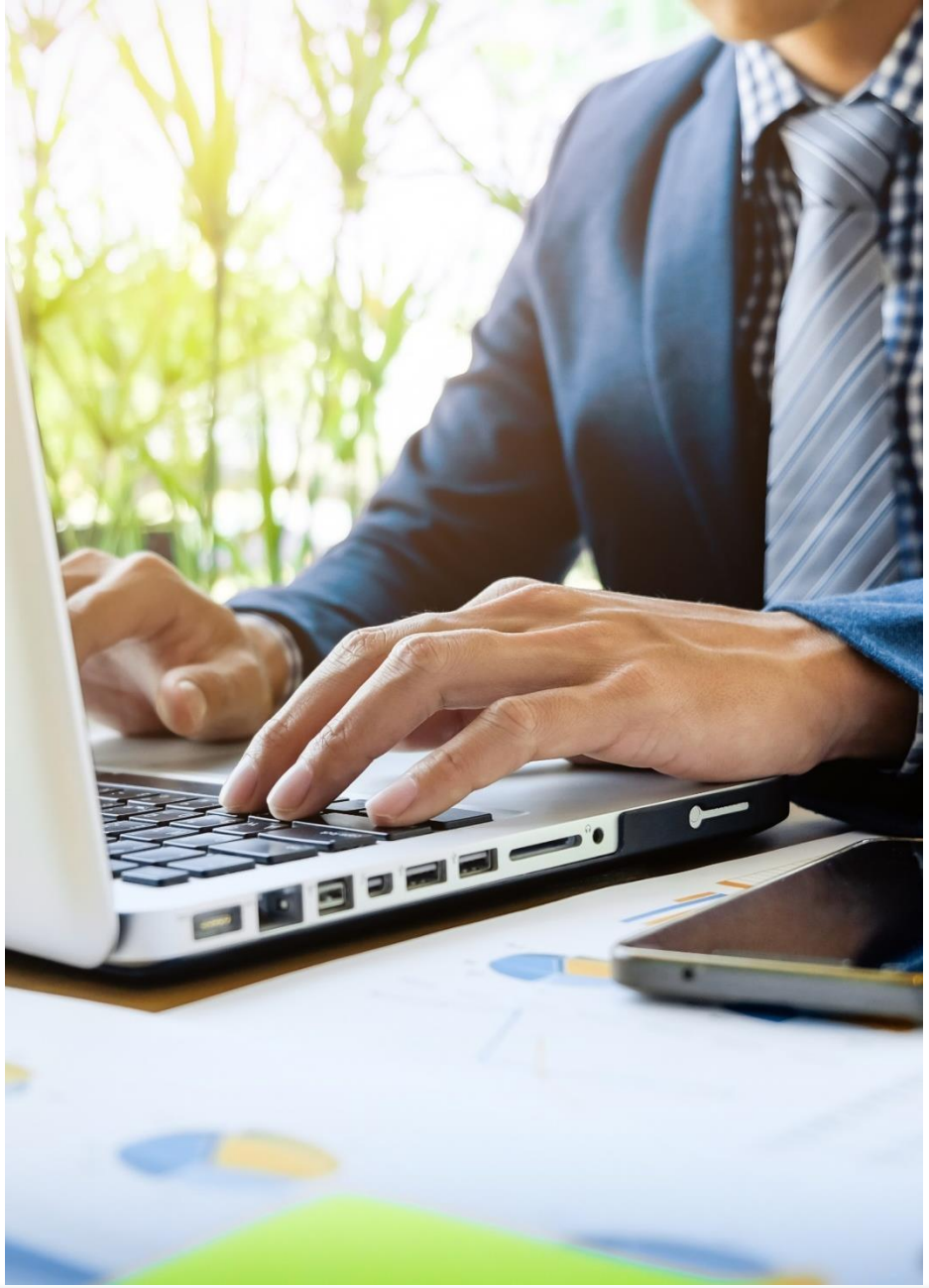
Da € 10.000 a € 50.000

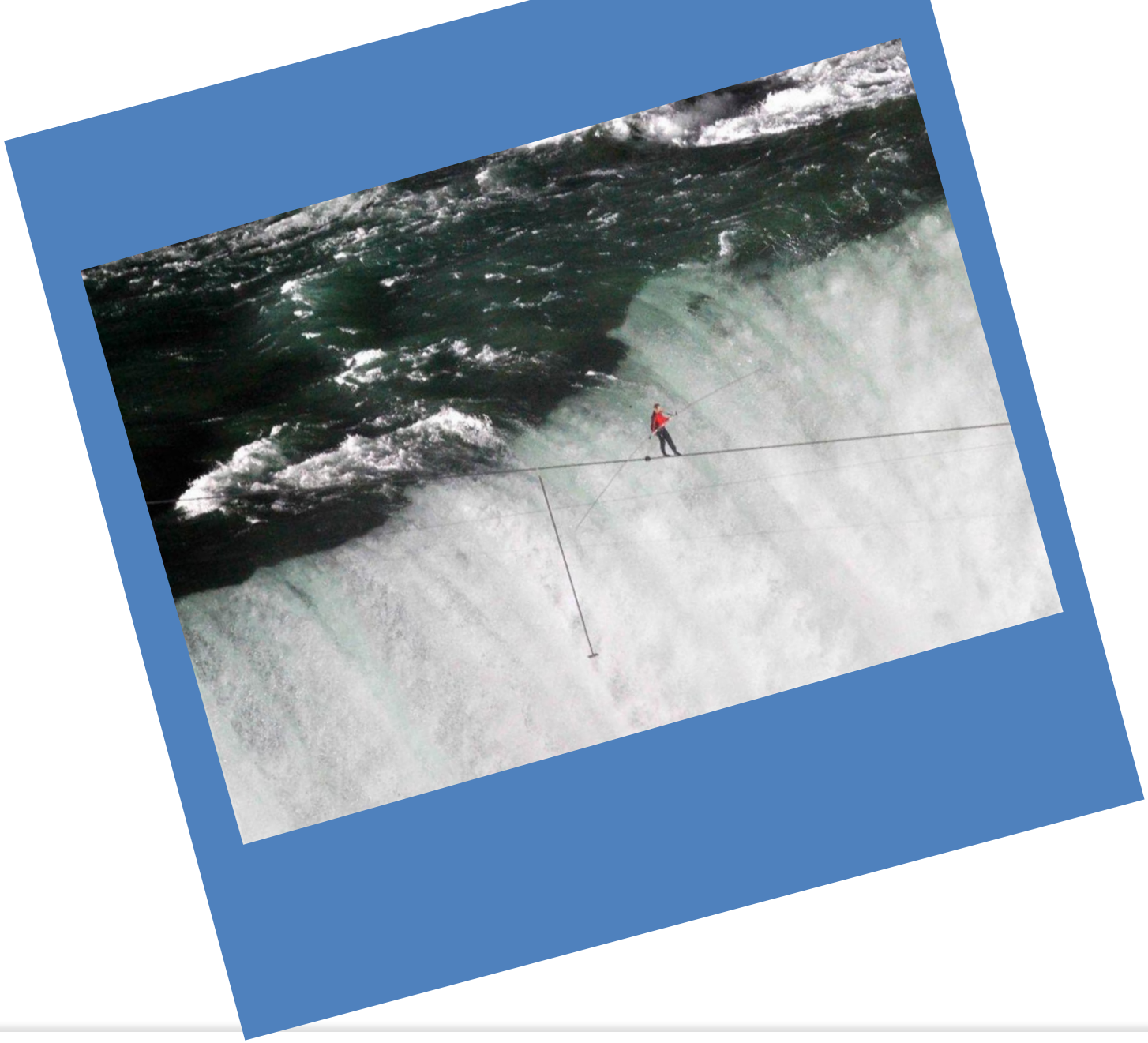
Per il mancato svolgimento da parte del responsabile di attività di verifica e analisi delle segnalazioni ricevute

La normativa: macigno o opportunità

Obiettivo del software? Tradurre la complessità in opportunità

- **Legge «0» di Asimov: un robot** *(..o un software NdR)* **non può recare danno all'umanità, né può permettere che, a causa del proprio mancato intervento, l'umanità riceva danno**
- Il compito della tecnologia deve essere quello di riassumere la complessità della norma e delle disposizioni collegate in uno strumento di lavoro facile, accessibile e sempre aderente alla norma





CINQUE SFIDE

1 - Tutela della riservatezza

Tutela della riservatezza del segnalante e del segnalato

- *Art. 54bis comma 5 Dlgs 165/2001*
- *Linee Guida ANAC*

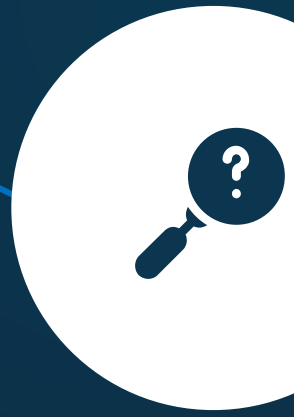
1 - TUTELA DELLA RISERVATEZZA

Esigenza

- Compliance normativa
- Aderenza anche se non si possiede una struttura informatica

Criticità

- Indispensabile una piattaforma informatica
- Crittografia
- Infrastruttura e sicurezza applicativa



Soluzione

Netta separazione del processo di iscrizione dal processo di segnalazione, per una corretta separazione dei dati a tutela dell'identità del segnalante

2 - Il ruolo di RPCT, ODV

- *Riceve e prende in carico le segnalazioni*

- *Pone in essere gli atti necessari ad una prima "attività di verifica e di analisi delle segnalazioni ricevute", da ritenersi obbligatoria in base al comma 6, dell'art. 54-bis*

2 - Il ruolo di RPCT, ODV

Esigenza

Assolvere a tutte le funzioni previste dalla norma

Criticità

- Complessità dell'istruttoria
- Coinvolgimento dei collaboratori

Soluzione

Gestione dedicata per RPCT, ODV e Collaboratori

Assegnazione automatica delle segnalazioni ai responsabili in base alla tipologia

Interazione con soggetti terzi rispetto al segnalante e al responsabile

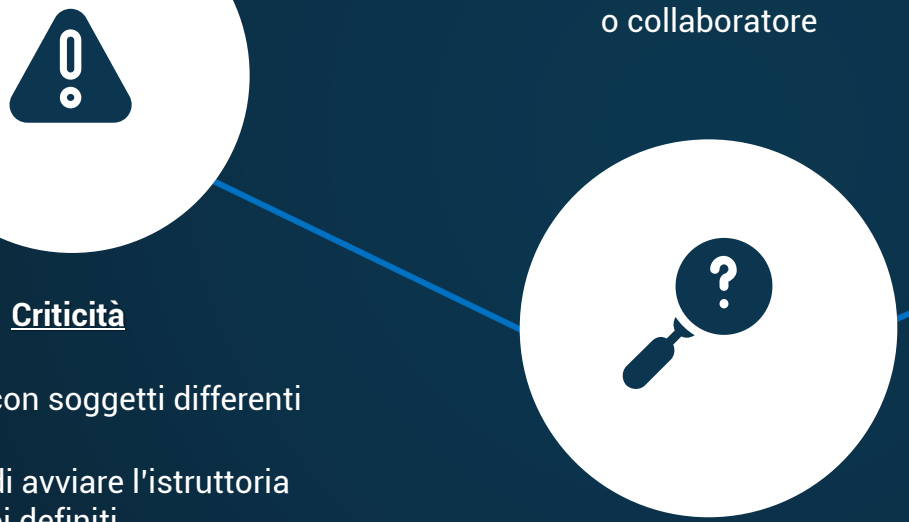
3 - LA GESTIONE DELLE SEGNALAZIONI

La legge 179 assegna al RPCT un ruolo fondamentale nella gestione delle segnalazioni. Il RPCT oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari ad una prima “attività di verifica e di analisi delle segnalazioni ricevute", da ritenersi obbligatoria in base al co. 6, dell'art. 54-bis19 pena le sanzioni pecuniarie dell'Autorità (commi 1 e 6, art. 54-bis)

3 - LA GESTIONE DELLE SEGNALAZIONI

Esigenza

Svolgere correttamente la propria mansione di RPCT, ODV o collaboratore



Criticità

- Dialogo con soggetti differenti
- Obbligo di avviare l'istruttoria con tempi definiti
- Riservatezza

Soluzione

Il sistema informatico deve essere customizzabile in base alle esigenze dell'organizzazione

4 - POLITICHE DI SICUREZZA

- *Modalità di conservazione dei dati*

- *Tutela della riservatezza attraverso strumenti informatici: disaccoppiamento dei dati del segnalante rispetto alle informazioni relative alla segnalazione, crittografia dei dati e dei documenti allegati*

- *Tempo di conservazione*

- *Politiche di sicurezza es. modifica periodica delle password*

4 - POLITICHE DI SICUREZZA

Esigenza

Dotarsi di uno strumento certificato e REALMENTE SICURO

Criticità

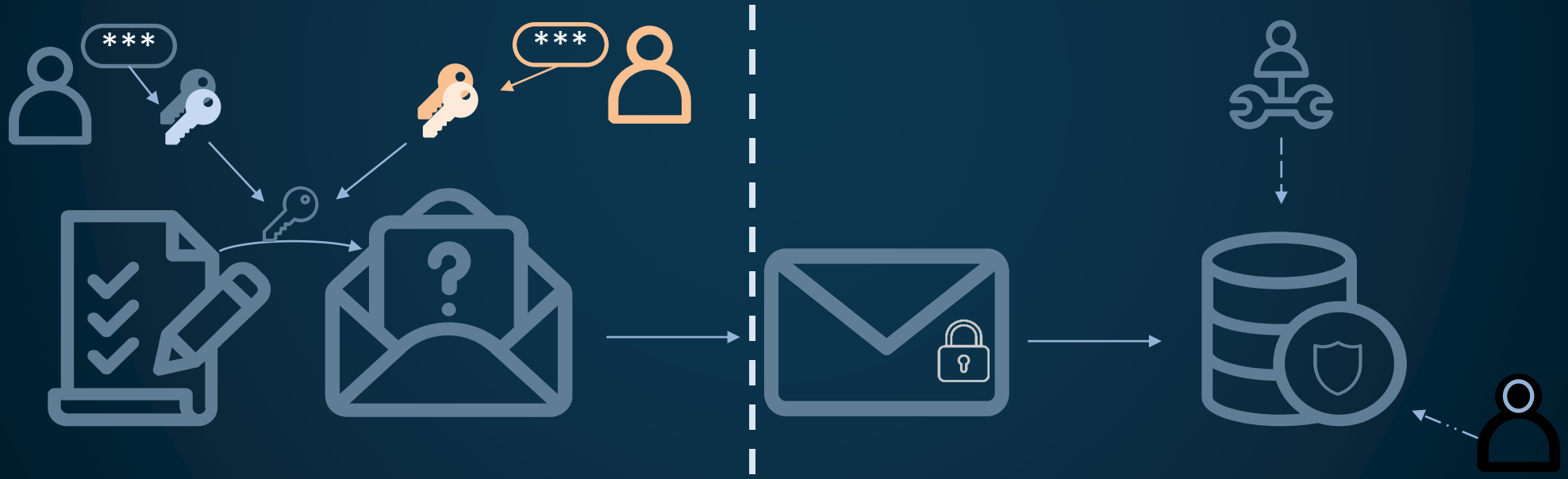
Obiettiva difficoltà del rispetto delle disposizioni senza uno strumento adeguato e aggiornato

Soluzione

Sicurezza e riservatezza lato Software

4 - POLITICHE DI SICUREZZA – LATO SOFTWARE

Come e da chi viene gestito e conservato il dato?
Come vengono gestite la riservatezza e la sicurezza?



5 - AGGIORNAMENTO NORMATIVO

La manutenzione e la costante compliance normativa devono essere un punto fondamentale per ogni organizzazione e per il fornitore

5 - AGGIORNAMENTO NORMATIVO

Criticità

- Soluzioni ospitate in casa
- Mancanza di expertise interna sia tecnica che normativa

Esigenza

Disporre sempre di una piattaforma rispondente alle normative vigenti in quello specifico momento

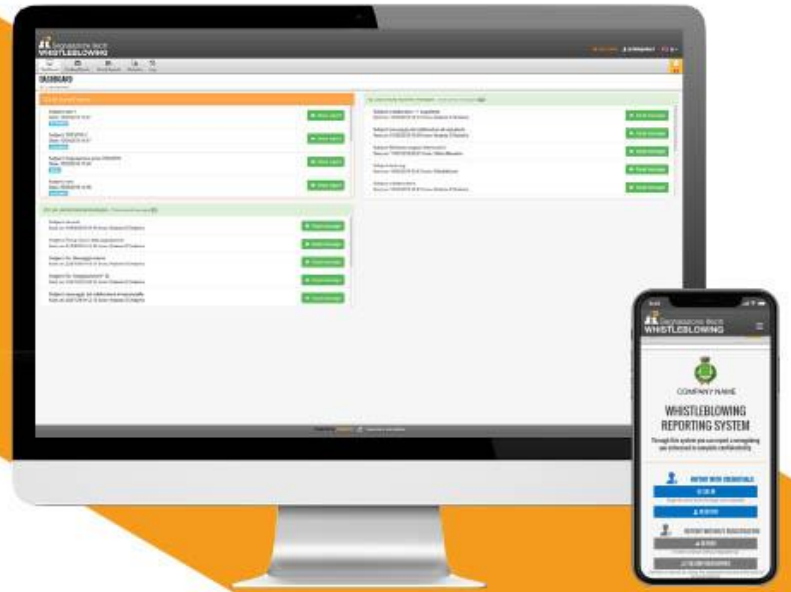
Soluzione

Segnalazioni.net è lo strumento informatico che consente agli operatori del settore Pubblico o Privato di effettuare segnalazioni di illeciti con la garanzia di un costante aggiornamento normativo

Segnalazione Illeciti
WHISTLEBLOWING

Segnalazioni.net è la piattaforma certificata AGID e software di riferimento del Whistleblowing.

Consente agli operatori del settore pubblico o privato di effettuare segnalazioni di illeciti con la garanzia di estrema riservatezza, certificata dai più rigorosi standard della norma ISO/IEC 27001.



Accessibile
e multidispositivo (pc, tablet e smartphone)

Sicuro
crittografia asimmetrica su contenuti e file allegati

Personalizzabile
contenuti, informative e privacy

DIGITALPA
Software & Servizi per PA e Aziende

GRUPPOSTRAZZERI
KNOWLEDGE SHARING

Asso 231
STAKEHOLDERS A CONFRONTO

GIACC ITALY
Global Infrastructure Anti-Corruption Centre

Anti Bribery ACADEMY

Segnalazione Illeciti
WHISTLEBLOWING

Riservatezza
Iter di registrazione separato dal processo di segnalazione e possibilità di gestire le segnalazioni di utenti non registrati

GDPR
Accesso regolamentato a norma GDPR (Regolamento Europeo 679/2016)

Profilo utenti
Gestione dedicata per RPCT, ODV e Collaboratori

Configurazione
Erogabile in configurazione per Aziende Private, Società Partecipate ed Enti Pubblici

Automatismi
Assegnazione automatica delle segnalazioni per tipologia

Multiente e multilingua
Versione disponibile per gruppi di società e possibilità di fruire del sito in altre lingue

Grazie per l'attenzione!

Domande?

DigitalPA S.r.l.
Via San Tommaso d'Aquino, 18 A – 09134 Cagliari (CA)
Tel. 070 349 5386

info@digitalpa.it
digitalpa@pec.it