

**20  
25**



**Compliance**

---

## **Whistleblowing**

Nuovi obblighi dal 2023 anche per le aziende private



Compliance

[info@compliance-srl.it](mailto:info@compliance-srl.it)  
[whistleblowing@compliance-srl.it](mailto:whistleblowing@compliance-srl.it)

---

[www.compliance-srl.it](http://www.compliance-srl.it)

---

Dott. Daniel Zisa  
+39 338 1623 958

---

In attuazione della Direttiva (UE) 2019/1937, è stato emanato il D.Lgs. n. 24 del 10 marzo 2023 riguardante la protezione delle persone che segnalano violazioni alla normativa nazionale o comunitaria.



Il Decreto è entrato in vigore il 30 marzo 2023 e le disposizioni ivi previste sono efficaci dal 15 luglio 2023.

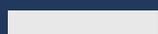


Il Decreto si applica ai soggetti del settore privato che hanno impiegato, nell'ultimo anno, la media di almeno **cinquanta lavoratori** subordinati o, anche sotto tale limite, agli enti che si occupano di particolari **settori sensibili** (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente), nonché a quelli che **hanno adottato un Modello di Organizzazione, Gestione e Controllo** ai sensi del D.Lgs. 231/2001.



# DECORRENZA

Per le aziende che hanno avuto nell'ultimo anno una media superiore a 249 dipendenti l'obbligo di istituire un apposito canale per la gestione delle segnalazioni di illeciti (Whistleblowing) entra in vigore il 15 luglio 2023. Per le aziende che hanno avuto tra i 50 ed i 249 dipendenti o comunque abbiano deliberato un Modello ex D.Lgs. 231/2001 l'entrata in vigore è il 17 dicembre 2023.



Situazione	Obbligo dal
Numero dipendenti superiore a 249	15 luglio 2023
Numero dipendenti da 50 a 249	17 dicembre 2023
Presenza del Modello Organizzativo 231/2001	17 dicembre 2023



# QUALI OBBLIGHI ENTRANO IN VIGORE A TALI SCADENZE

---

- ➔ **DOTARSI** di una piattaforma di segnalazione sicura conforme alla normativa, che protegga la riservatezza dell'identità e i dati personali di chi denuncia condotte illecite. Le imprese dovranno, quindi, predisporre propri canali di segnalazione interna e gestire le segnalazioni ricevute tramite software che utilizzano sistemi crittografici, capaci di garantire la riservatezza dell'identità di chi segnala, della persona coinvolta e del contenuto della segnalazione stessa, nonché dei relativi documenti di supporto.
- ➔ **GARANTIRE**, attraverso un sistema criptato, al segnalante che voglia rimanere anonimo la possibilità di instaurare un filo diretto con un "Facilitatore", inviando informazioni in merito a una condotta illecita, alle circostanze che l'hanno prodotta e alle persone coinvolte.
- ➔ **IMPLEMENTARE** una struttura adeguata a ricevere ed esaminare le possibili segnalazioni trasmesse dai segnalanti (Whistleblower), che possono essere, oltre che dipendenti dell'organizzazione, anche collaboratori autonomi quali liberi professionisti o consulenti della società, volontari e tirocinanti anche non retribuiti, azionisti/soci, ecc.



L'ente autonomo (requisito che ANAC ha declinato come imparzialità e indipendenza) che riceve la segnalazione potrà essere interno all'azienda (solo se presenti organi di internal audit, Organismo di vigilanza previsto dalla disciplina del D.Lgs. n. 231/2001 o comitati etici) o esterno, e dovrà essere adeguatamente formato garantendo il requisito di protezione dell'identità del soggetto segnalante. Il cosiddetto "facilitatore" dovrà:

- ➔ ricevere ed esaminare la fondatezza delle segnalazioni pervenute;
- ➔ assicurare una efficiente e tempestiva gestione delle segnalazioni;
- ➔ rilasciare alla persona segnalante un avviso di ricevimento della segnalazione entro sette giorni dalla data di invio;
- ➔ prendere e mantenere contatti con il segnalante al fine di approfondire la notizia ed acquisire tutti gli elementi di prova utili per i successivi approfondimenti e sviluppi;
- ➔ implementare un sistema di reporting attraverso i quali veicolare le segnalazioni ai soggetti preposti (es. CdA), sempre nel rispetto della riservatezza del soggetto segnalante, salvo diversa volontà dello stesso;
- ➔ conservare e custodire la documentazione inerente ciascuna segnalazione nei termini previsti dalla normativa vigente.





# OGGETTO DELLE SEGNALAZIONI

Potranno essere oggetto di segnalazione i comportamenti o le omissioni lesivi dell'interesse pubblico, dell'integrità dell'Amministrazione o dell'azienda privata, riguardanti:

illeciti civili;

illeciti penali;

illeciti amministrativi e contabili;

illeciti rientranti nell'ambito dei reati presupposto di cui al decreto legislativo n. 231/2001 o violazione dei modelli di organizzazione e gestione;

illeciti commessi in violazione della normativa dell'UE e di tutte le disposizioni nazionali che ne danno attuazione;

atti od omissioni lesivi degli interessi finanziari dell'Unione Europea o del mercato interno.

Sarà possibile segnalare le condotte illecite qualora vi sia un ragionevole e fondato motivo di ritenere che le informazioni in proprio possesso siano vere e rientrino nell'ambito della normativa.

# LE SANZIONI PER CHI NON SI ADEGUA



Il Decreto Legislativo n. 24, pubblicato in Gazzetta Ufficiale il 15 marzo 2023, prevede, tra le diverse misure, la sanzione **da 10.000 a 50.000 euro** nei confronti dei soggetti che:

- ➔ non hanno istituito canali di segnalazione adeguati;
- ➔ non hanno adottato procedure per l'effettuazione e la gestione delle segnalazioni;
- ➔ non hanno adottato procedure conformi a quelle richieste dalla legge;
- ➔ non hanno svolto l'attività di verifica e analisi delle segnalazioni ricevute.

L'Autorità competente per la vigilanza del corretto adempimento degli obblighi di cui sopra e per l'irrogazione delle relative sanzioni è l'ANAC (Autorità Nazionale per l'Anticorruzione).

# LA NOSTRA OFFERTA



---

**01**

Creazione di uno specifico “canale di allerta aziendale” nella piattaforma applicativa per la gestione delle segnalazioni interne come richiesto dal D.Lgs. 24/2023.

**02**

Creazione e condivisione del link aziendale che permetta al lavoratore / soggetto terzo di inviare la segnalazione e seguire i successivi sviluppi.

**03**

Supporto nell'elaborazione della documentazione necessaria da pubblicare sulla pagina web dedicata.

**04**

Creazione e condivisione di materiale (es. slide, flyer/volantini, etc.) per permettere all'azienda cliente di adempiere all'obbligo di informazione / formazione aziendale sull'argomento.

**05**

Creazione e/o collaborazione nell'aggiornamento costante della Procedura aziendale contenente le modalità di allerta secondo la normativa Whistleblowing.

06

Conformità al GDPR/normativa privacy (elaborazione informative sul trattamento dei dati, supporto integrazione Registro dei Trattamenti, nomina Responsabili e consegna della Valutazione d'impatto sulla protezione dei dati - DPIA).

07

Consegna annuale del Vulnerability Assessment che garantisce gli elevati standard di sicurezza informatica del Data Center in cui i dati sono archiviati.

08

Gestione dell'allerta ricevuta con riscontro al soggetto segnalante (es. richiesta di ulteriori informazioni, di evidenze fotografiche, documenti ecc.).

09

Invio immediato del "Report di Allerta" ai soggetti apicali aziendali nel caso la segnalazione sia credibile e di entità rilevante (in base a quanto definito dalle policy aziendali e dalle linee guida ANAC).

10

Creazione di reportistica, consegnata periodicamente alla Società cliente (Relazione trimestrale sulle allerte ricevute).



# ALTRI SERVIZI OFFERTI



**Consulenza Modelli Organizzativi 231/2001**



**Assistenza Organismi di Vigilanza (OdV)**



**Consulenza GDPR/ Privacy**



**Attività di Data Protection Officer (DPO)**



**Sistemi di Gestione ISO**



**Internal Auditing**



Compliance

# RIFERIMENTI E CONTATTI

[info@compliance-srl.it](mailto:info@compliance-srl.it)  
[whistleblowing@compliance-srl.it](mailto:whistleblowing@compliance-srl.it)

---

[www.compliance-srl.it](http://www.compliance-srl.it)

---

Dott. Daniel Zisa  
+39 338 1623 958

---