Dopo una lunga gestazione e plurimi rinvii, mercoledì 15 marzo 2023 è stato pubblicato in G.U. il Decreto Legislativo 10 marzo 2023, n. 24 di recepimento della Direttiva (UE) 2019/1937, in vigore dal prossimo 30 marzo 2023 (di seguito, “Decreto Whistleblowing” o “Decreto”).

Il Decreto Whistleblowing avrà un IMPATTO SIGNIFICATIVO E IMMEDIATO nell’organizzazione delle imprese.

L’implementazione obbligatoria di canali di segnalazione richiederà di considerare con estrema attenzione una molteplicità di temi strettamente connessi di corporate governance, risk management, protezione dei dati personali e diritti dei lavoratori.

L’attivazione di un sistema di whistleblowing è un tema di governance e compliance abilitante e qualificante anche sotto il profilo ESG, concorrendo significativamente al perseguimento di target riconducibili a molteplici obiettivi dell’Agenda 2030 per lo Sviluppo Sostenibile.

Rispondiamo – senza alcuna pretesa di completezza - ad alcune primissime domande.

Qual è lo scopo del Decreto Whistleblowing?

Il Decreto Whistleblowing ha lo scopo di tutelare le persone che segnalano violazioni di disposizioni normative nazionali o dell’Unione Europea che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato, di cui siano venute a conoscenza nel proprio contesto lavorativo.

La tutela non si applica:

1. alle contestazioni, rivendicazioni o richieste legate ad un interesse di carattere esclusivamente personale del segnalante;
2. alle segnalazioni di violazioni già disciplinate in via obbligatoria dagli atti dell’Unione Europea o nazionali;
3. alle segnalazioni di violazioni in materia di sicurezza nazionale, appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell’Unione Europea.

Come possono essere trasmesse le segnalazioni?

Le segnalazioni possono essere trasmesse attraverso:

1. canali di segnalazione interna https://anonymousemail.me;
2. canale di segnalazione esterna, attivato dall’Autorità Nazionale Anticorruzione (ANAC) https://www.anticorruzione.it/-/segnalazioni-contratti-pubblici-e-anticorruzione
3. divulgazioni pubbliche, tramite i mass media.

Modulo per la segnalazione delle violazioni:

www.pergamosrl.it/_files/ugd/9d4295_fcfc16185f23413abb98b0b789d1c4c3.pdf

Quali sono i soggetti obbligati nel settore privato?

Nel settore privato, l’obbligo di implementare canali di segnalazione, adottare procedure per l’effettuazione e la gestione delle segnalazioni, e garantire le misure di tutela si applica agli enti privati (incluse le società) che:

1. nell'ultimo anno, hanno impiegato la media di almeno 50 lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato, a prescindere dal settore di appartenenza;
2. hanno adottato un modello organizzativo ai sensi del D. Lgs. 231/2001 ("Modelli 231"), a prescindere dal numero dei dipendenti impiegati e dal settore di appartenenza;
3. rientrano nell'ambito di applicazione degli atti dell'Unione Europea – elencati nell'allegato al Decreto - in materia di servizi, prodotti e mercati finanziari, prevenzione del riciclaggio e finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente, a prescindere dal numero dei dipendenti impiegati.

Si precisa che i gruppi le cui imprese hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a 249, possono condividere il canale di segnalazione interna e la relativa gestione.

Qual è la scadenza per gli enti privati?

L'obbligo di implementare i canali di segnalazione scatta:

- dal 15 luglio 2023, per gli enti privati con 250 o più dipendenti;
- dal 17 dicembre 2023 per i soggetti privati con 50 o più dipendenti.

Chi sono i segnalanti / whistleblower tutelati?

Il Decreto Whistleblowing amplia in modo significativo il novero dei soggetti tutelati in caso di segnalazione comprendendo, oltre ai dipendenti: lavoratori autonomi; liberi professionisti e consulenti; volontari e tirocinanti; azionisti e persone con funzioni di amministrazione, direzione, controllo e vigilanza o rappresentanza; candidati; lavoratori in prova; ex dipendenti; facilitatori; parenti o colleghi di lavoro del segnalante; enti di proprietà del segnalante o che operano nel medesimo contesto lavorativo del segnalante.

Quali sono le misure di protezione previste?

Chi, alle condizioni previste dal Decreto, effettua la segnalazione:

- è protetto dal divieto di ritorsioni, anche indirette, nei suoi confronti (tra cui, licenziamento, sospensione, retrocessione di grado o mancata promozione, demansionamento, referenze negative, intimidazioni o molestie, danni reputazionali, ecc.);
- beneficia di misure di sostegno fornite da enti del Terzo settore (ovvero, informazioni, assistenza e consulenze a titolo gratuito sulle modalità di segnalazione e sulla protezione dalle ritorsioni, sui diritti della persona coinvolta, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato).

Quali sono le sanzioni applicabili?

Fermi restando gli altri profili di responsabilità, l'ANAC applica al responsabile sanzioni amministrative pecuniarie fino a 50.000 euro quando accerta, tra l'altro, che:

- sono state commesse ritorsioni;
- la segnalazione è stata ostacolata/si è tentato di ostacolarla;
- è stato violato l'obbligo di riservatezza;
- non sono stati istituiti canali di segnalazione;
- non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni o le procedure adottate non sono conformi al Decreto;
- non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute.

Cosa fare subito?

PUNTO PRIMO: ISTITUIRE DEI CANALI DI SEGNALAZIONE | COMPLIANCE

I soggetti obbligati, sentite le rappresentanze o le organizzazioni sindacali, devono implementare propri canali di segnalazione che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

In particolare, gli enti e le società dotati di Modelli 231 dovranno adeguare i canali di segnalazione già adottati, in modo da armonizzarne l'utilizzo ai più ampi fini del Decreto Whistleblowing.

PUNTO SECONDO: ORGANIZZARE LA GESTIONE DEI CANALI DI SEGNALAZIONE | GOVERNANCE

Tema prioritario è quello della governance delle segnalazioni. La gestione dei canali di segnalazione deve essere regolamentata con una procedura e affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione o a un soggetto esterno.

Attenzione: il Decreto Whistleblowing prevede che le segnalazioni possano essere effettuate in forma scritta, anche (e quindi, non solo) con modalità informatiche, oppure in forma orale, attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole.

A tal riguardo, le piattaforme tecnologiche possono offrire un prezioso supporto per la gestione organizzata delle segnalazioni ma non esauriscono il tema whistleblowing che deve essere invece affrontato e governato nell'osservanza di tutte le leggi applicabili e con una visione ispirata a criteri ESG.

PUNTO TERZO: APPLICARE MISURE DI DATA PROTECTION E CYBER SECURITY | DATA PROTECTION E CYBER SECURITY

Rispetto agli adempimenti data protection, i titolari del trattamento sono chiamati ad applicare una serie di misure di natura sia organizzativa sia tecnica, al fine di tutelare la riservatezza del segnalante e l'integrità, nonché la confidenzialità, dei dati personali oggetto di segnalazione.

L'evidenza di tali prescrizioni è indicata all'art. 13 del Decreto, rubricato «Trattamento di dati personali», il quale richiama espressamente il rispetto dei princìpi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 ("GDPR") e di privacy by design e by default.

Un'attenzione particolare dovrà essere riservata all'approccio risk based rispetto all'obbligo di svolgimento dell'attività di analisi dei rischi e di valutazione degli impatti data protection, tenuto conto altresì del termine di conservazione dei dati oggetto di trattamento individuato nei 5 anni successivi alla data di comunicazione dell'esito finale della procedura di segnalazione.

Contestualmente, dovrà essere assicurata anche la sicurezza del canale di segnalazione in termini di confidenzialità, integrità e disponibilità delle informazioni, sia per quel che concerne l'oggetto della segnalazione che i dati personali del segnalante.

PUNTO QUARTO: INFORMARE E SENSIBILIZZARE | GOVERNANCE, COMPLIANCE, SOSTENIBILITÀ

Le imprese devono informare e sensibilizzare dipendenti e terzi interessati attraverso politiche di whistleblowing che definiscano in modo semplice e comprensibile le finalità e modalità di utilizzo dei canali di segnalazione.

Le imprese devono diffondere una cultura delle segnalazioni come strumento di compliance, responsabilità sociale e sostenibilità.