GLOBAL QUALITY

WHISTLEBLOWING

Le novità introdotte dal D.Lgs. 24/2023 in attuazione della Direttiva (UE) 2019/1937

03/2023

1 Il D.lgs. 24/2023 “Whistleblowing”

Il 15/03/2023 con la pubblicazione in Gazzetta Ufficiale del D.lgs. 24/2023, l’Italia ha recepito la Direttiva 2019/1937 del Parlamento europeo e del Consiglio in tema di protezione delle persone che segnalano violazioni del Diritto dell’Unione e violazioni delle disposizioni normative nazionali, c.d. (“whistleblowing”). Il Decreto garantisce un elevato livello di protezione di coloro che segnalano minacce o pregiudizi al pubblico interesse di cui sono venuti a sapere nell’ambito delle loro attività professionali, estesa a tutti i soggetti collegati all’organizzazione e/o alla persona del segnalante.

1.1 Applicazione

Il decreto trova applicazione nei confronti

- dei soggetti privati che nell’ultimo anno hanno impiegato almeno 50 lavoratori;
- dei soggetti privati che, indipendentemente dal numero di addetti, hanno adottato un Modello di organizzazione gestione e controllo ex d.lgs. 231/2001;
- dei soggetti operanti in specifici settori e nei confronti dei soggetti pubblici.

Il D.lgs. 24/2023 si applica alle segnalazioni di violazioni, (i.e. di comportamenti, atti od omissioni) che ledono l’interesse pubblico o l’integrità dell’amministrazione pubblica o dell’ente privato e che consistono in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del D.lgs. 231/2001, o violazioni dei modelli di organizzazione e gestione;
- illeciti che rientrano nell’ambito di applicazione di discipline normative unionali o nazionali degli atti dell’Unione europea o nazionali,

1.2 Tipologie di segnalazioni

Il Decreto prevede tre “canali” di segnalazione a disposizione dei whistleblower:

1. Interna, gestita dalla Società;
2. esterna (gestito da ANAC);
3. divulgazione pubblica.

In particolare, la persona segnalante può effettuare una segnalazione esterna se, al momento della sua presentazione, il canale di segnalazione interna non è attivo o, anche se attivato, non è conforme a quanto previsto dalla normativa.

1.3 Il canale di segnalazione interna

Per quanto riguarda i canali interni, è richiesto alle Società, sentite le rappresentanze o le organizzazioni sindacali, di istituire canali per ricevere le segnalazioni, progettati, realizzati e gestiti in modo tale da garantire la riservatezza dell’identità del segnalante e la protezione degli eventuali terzi citati nella segnalazione. La gestione del canale interno deve essere affidata a un ufficio interno autonomo dedicato, ovvero a un soggetto esterno autonomo, sempre specificamente formato.

Le segnalazioni possono essere effettuate:

- in forma scritta, anche con modalità informatiche;
- in forma orale attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto.

Il decreto definisce tempistiche precise per la gestione della segnalazione: avviso di ricevimento della segnalazione entro 7 giorni dalla data di ricezione; riscontro alla segnalazione entro 90 giorni.

1.4 Entrata in vigore del Decreto

- 15 luglio 2023: per le società con più di 250 dipendenti.

- 17 dicembre 2023: per le società del settore privato da 50 fino a 249 dipendenti, ovvero dotate di Modello di organizzazione gestione e controllo ex d.lgs. 231/2001.

1.5 Tutela della riservatezza e trattamento dei dati

Vengono definiti chiari requisiti per la tutela della riservatezza e trattamento dei dati:

- i dati personali che non sono utili al trattamento della segnalazione vanno cancellati immediatamente;
- il canale interno implementato per la gestione delle segnalazioni deve essere sottoposto a Valutazione di impatto ai sensi dell'art. 35 del Reg. UE n. 2016/679 (GDPR);
- la conservazione dei dati non deve andare oltre i 5 anni.

1.6 Sanzioni

Tra le sanzioni amministrative pecuniarie stabilite dal decreto, è prevista una sanzione da €10.000 a €50.000 quando non sono stati istituiti canali di segnalazione, ovvero non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni ovvero che l'adozione di tali procedure non è conforme ai requisiti, nonché quando accerta che non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute.

2 Implementazione e gestione del processo Whistleblowing

Le fasi di implementazione del processo aziendale di segnalazione Whistleblowing, analisi e gestione delle segnalazioni ricevute, in linea con quanto richiesto dalla normativa, sono le seguenti:

1 definizione del processo di gestione delle segnalazioni, individuando e valutando le migliori soluzioni organizzative, anche in contesti di Gruppi di Società;
2 implementazione di un idoneo canale di segnalazione informatico;
3 redazione di policy e procedure aziendali per la gestione del Whistleblowing;
4 attuazione degli adempimenti previsti in merito alla protezione dei dati personali;
5 erogazione di interventi formativi in tema di Whistleblowing;
6 gestione della compliance in tema di trattamento dei dati personali, attraverso:
   - ✓ valutazione d'impatto del trattamento (DPIA);
   - ✓ la redazione dell'Informativa privacy aggiornata al trattamento;
   - ✓ l'integrazione del registro dei trattamenti;
   - ✓ la nomina ad autorizzato del trattamento
7 gestione delle segnalazioni ricevute, inteso come:
   - ✓ raccolta/ricezione delle segnalazioni ricevute;
   - ✓ valutazione preliminare delle segnalazioni ricevute;
   - ✓ svolgimento (o supporto) di attività di investigazione;
   - ✓ suggerimento di azioni rimediali.

Caratteristiche dell'app per la gestione delle segnalazioni in SAAS

- software SAAS per la gestione delle segnalazioni, multilingua e multicanale;

La piattaforma offerta si basa su Globaleaks, software opensource a supporto del whisteblowing. Il software implementa by design e by default le più appropriate configurazioni in materia di sicurezza, protezione di dati e anonimato.

Il software è riconosciuto come un Digital Public Good dalla Digital Public Goods Alliance ed viene raccomandato da Transparency International oltre che dall'autorità nazionale anticorruzione ANAC, che lo ha adottato per la gestione del proprio canale Whistleblowing.

Il software viene offerto in configurazione **Standard** o **Premium** in base alle necessità aziendali.

Di seguito vengono riportate le caratteristiche del software stesso:

Caratteristiche funzionali:	Standard	Premium
Interamente gestibile da un'interfaccia di amministrazione web	✓	✓
Gestione e pianificazione di scadenze, gestione della documentazione e reportistica	✓	✓
Aspetto grafico personalizzabile (logo, testo)	✓	✓
Scambio di file multimediali con l'informatore	✓	✓
Chat con l'informatore per discutere della segnalazione	✓	✓
Ricerca e statistiche delle segnalazioni	✓	✓
Categorizzazione dei report con etichette	✓	✓
Supporto per più di 90 lingue con supporto per Right-to-Left (RTL)		✓
Creazione di workflow e stati personalizzati per la gestione dei casi		✓
Creazione di questionari personalizzati		
Supporto autenticazione a due fattori (2FA) conforme allo standard TOTP RFC 6238		✓

Caratteristiche legali

- Conforme alla norma ISO 37002 e alla Direttiva UE 2019/1937;
- Politiche di conservazione dei dati configurabili;
- Nessun registro degli indirizzi IP.

Caratteristiche di sicurezza

- Registrazione dei certificati digitali (Let's Encrypt);
- Test di penetrazione multipli con report completi;
- Conformità agli standard di settore e alle best practice per la sicurezza delle applicazioni seguendo le linee guida sulla sicurezza OWASP;
- Non lascia tracce nella cache del browser;
- Protezione completa contro gli invii automatici (prevenzione dello spam);
- Supporto PGP per notifiche e-mail crittografate.

Caratteristiche tecniche

- Installazione su server in cloud di Cloud Provider con il quale è stato sottoscritto debito Accordo sul trattamento dei dati personali ex art. 28 del Reg. UE n. 2016/679 (GDPR);
- Piano di supporto a lungo termine (LTS);
- Applicazione completamente autonoma (non sono necessari server Web o applicazioni);
- Costruito con tecnologie framework leggere (AngularJS e Python Twisted) e Database – SQLite;
- Configurazione automatica di Tor Onion Services Versione 3;
- Backup integrato;
- Supporto HTTP/2.