



LA NUOVA DISCIPLINA DEL WHISTLEBLOWING

Decreto Legislativo 10 marzo 2023, n. 24

Il D. Lgs. 24/2023, di recepimento della direttiva 2019/1937, ha introdotto nell'ordinamento italiano una nuova disciplina dell'istituto del Whistleblowing, modificando in vari punti la precedente.

Cambiano, in particolare: il numero dei soggetti obbligati alla tutela del whistleblower; la tipologia dei reati da segnalare (inserendo per esempio anche la tutela dei dati personali); i soggetti tutelati dalla disciplina e prevedendo un sistema sanzionatorio anche in capo ad ANAC.

OGGETTO	NOVITÀ
Adozione di un sistema di whistleblowing	Diventa obbligatorio per: • PA (e assimilate); • società con una media annua di almeno 50 dipendenti; • società che operano nel settore di servizi, prodotti e mercati finanziari, prevenzione del riciclaggio o antiterrorismo (a prescindere dal numero di dipendenti) • società già munite di Modello 231 (a prescindere dal numero di dipendenti)
Soggetti tutelati	Segnalante, facilitatori, colleghi, parenti etc
Canali di segnalazione	Interni (da pubblicare sul sito, previo regolamento che lo disciplina) o tramite portale Anac. È obbligatorio adeguarsi alla disciplina sulle modalità di gestione della segnalazione, anche in ordine all'archiviazione. Vanno sentite le rappresentanze sindacali per eventuali osservazioni.
Sanzioni irrogate da ANAC	Da 10.000 a 50.000 euro in caso di mancata predisposizione del canale di segnalazione e di procedure per la gestione della segnalazione; ritorsioni, violazione del diritto alla riservatezza.
Sanzioni irrogate dal Garante Privacy	Fino a 20 milioni di euro
Entrata in vigore	• 15 luglio 2023 PA e società' con oltre 250 dipendenti; • 17 dicembre 2023 per i soggetti privati con oltre 50 dipendenti

AZIONI DA INTRAPRENDERE

Il 12 luglio 2023 ANAC ha deliberato le **Linee Guida per l'attuazione del decreto legislativo**, avendo ricevuto l'approvazione anche dal Garante per la Protezione dei Dati Personali.

Dalla lettura delle linee guida emergono gli **OBBLIGHI IN CAPO ALLA PA ED IMPRESE OBBLIGATE**:

1. **Creazione di un canale interno**, preferibilmente tramite piattaforme tecnologiche, per le segnalazioni, da rendere facilmente accessibile (es. pubblicandolo nel sito internet aziendale);
2. Sottoporre al fornitore della piattaforma una check list per la **verifica della conformità del software**. Le piattaforme tecnologiche dovranno garantire la sicurezza della segnalazione e la riservatezza del segnalante (es. usare canali https; crittografia e accessi limitati; verificare che il segnalante riceva solo un numero di segnalazione e non una mail automatica dal sito di conferma ricezione, al sito resta un indirizzo mail tracciato!) e la verifica è in capo al titolare. La riservatezza deve riguardare: l'identità del segnalante; il contenuto della segnalazione; la relativa documentazione.
3. Realizzare una **valutazione di impatto privacy** all'applicativo utilizzato ai sensi dell'art. 35 gdpr;
4. Redigere informative di trattamento specifiche sia ex art. 13 che ex art. 14 GDPR;
5. **Inserire il trattamento dei dati** relativo al Whistleblowing all'interno del registro dei trattamenti ex art. 30 gdpr;
6. **Individuare correttamente i soggetti coinvolti** e in tal senso:
 - nominare quale autorizzato al trattamento (ex art. 2 quaterdecies D. Lgs. 196/2003) il soggetto designato alla ricezione delle segnalazioni con specifici doveri di segretezza. Il nominato dovrà essere adeguatamente formato.
 - nominare responsabile del trattamento il fornitore del software, ed eventualmente subresponsabili se presenti.
 -
5. **definire le procedure interne per gestire le segnalazioni** (Regolamento sulla Gestione delle Condotte)
6. per le società che adottano modelli 231, rivedere il modello.

LA PROCEDURA E LA DPIA VANNO PUBBLICATE SUL SITO!!!

E' CONSENTITA L'ADOZIONE DI CANALI DI SEGNALEZIONE TRA PIU' SOGGETTI, ANCHE PRIVATI FINO A 249 DIPENDENTI. IN TALE CASO I SOGGETTI SONO CONSIDERATI CONTITOLARI

SANZIONI GIÀ COMMINATE



Data	7 aprile 2022
Importo Sanzione	€ 40.000
Titolare del Trattamento	Azienda ospedaliera di Perugia
Articoli violati	Art. 5, par. 1, lett. f) GDPR Artt. 13, 14, 25, 30, 32 e 35 GDPR

Dall'ingiunzione è emerso il **mancato assolvimento dell'obbligo di rendere informazioni agli interessati**.
La **mancata indicazione dei trattamenti per finalità di whistleblowing nel registro delle attività di trattamento**.
Mancanza di specifiche cautele al fine di non effettuare la registrazione delle operazioni di navigazione sull'applicazione web per l'acquisizione e la gestione di segnalazioni di condotte illecite.
Inoltre il **trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati**.





Data	10 giugno 2021
Importo Sanzione	€ 40.000
Titolare del Trattamento	Aeroporto Guglielmo Marconi di Bologna S.p.a.
Articoli violati	Art. 5, par. 1, lett. f) GDPR Artt. Artt. 25, 32 e 35 GDPR

Dall'ingiunzione è emerso il **mancato utilizzo della crittografia nella trasmissione e nella conservazione dei dati**, condotte quindi che più in generale riguardano la mancata applicazione dei principi di protezione dei dati per la tutela degli interessati (art. 5) ed osservanza del principio della privacy by design, quindi della "protezione dei dati fin dalla progettazione".
Inoltre Il **trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati**.





Data	23 gennaio 2020
Importo Sanzione	€ 30.000
Titolare del Trattamento	Università degli Studi di Roma "La Sapienza"
Articoli violati	Art. 5, par. 1, lett. a), GDPR Art. 32 GDPR

Dall'ingiunzione è emersa la **divulgazione dei nomi dei segnalanti sul web**. E' stato utilizzato un **protocollo di rete "http", privo di un sistema di crittografia**, per il trasporto dei dati, il quale non garantiva una **comunicazione sicura in termini di riservatezza e integrità dei dati scambiati**.
Il Garante ha precisato che Il **datore di lavoro**, nell'adozione di procedure tecnologiche per la segnalazione anonima di possibili comportamenti illeciti (whistleblowing), deve **verificare che le misure tecnico-organizzative e i software utilizzati siano adeguati a tutelare la riservatezza di chi invia le denunce**.

