Procedura sull'applicazione del decreto Lgs 24/2023 WHISTLEBLOWING
in materia di Privacy

Il nuovo **Dlgs 24/2023** mira a rafforzare la **protezione dei soggetti segnalanti, comunemente noti come "whistleblowers"**, che denunciano comportamenti, atti o omissioni dannosi per l'interesse pubblico o l'integrità dell'amministrazione pubblica o di enti privati.

I destinatari di questa normativa sono definiti nell'art. 3 del Decreto, e in particolare per quanto riguarda il settore privato, l'obbligo si applica *anche alle imprese che non hanno adottato un MOG231* (modello previsto dal Decreto Legislativo n. 231 del 2001), ma che soddisfano una delle seguenti condizioni:

- **impiego di almeno cinquanta lavoratori subordinati**, con contratti di lavoro a tempo indeterminato o determinato, nell'ultimo anno, oppure
- **operano in settori specifici** come servizi, prodotti e mercati finanziari, prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente, anche se nell'ultimo anno non hanno raggiunto la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato.

CANALE DI SEGNALAZIONE INTERNO

L'art. 6 del Decreto prevede l'attuazione di **misure di sicurezza per le comunicazioni interne**, con l'obbligo di garantire la **riservatezza del segnalante e delle persone coinvolte** anche attraverso l'utilizzo di **piattaforme informatiche dotate di sistemi di crittografia**.
Per la **gestione del canale di segnalazione interno**, deve essere designata una **persona o un ufficio autonomo specificamente formati**: la gestione del canale può anche essere **affidata ad un soggetto esterno** (fornitore).
La Dupont Energetica Spa ha affidata il canale di segnalazione interna al proprio Organismo di Vigilanza.
Per effettuare una segnalazione l'utente (Whistleblower) deve necessariamente collegarsi alla piattaforma informatica dove verrà guidato attraverso un percorso standard inserendo tutti i dati obbligatori previsti. **La piattaforma garantisce la sicurezza dei dati comunicati attraverso l'utilizzo della crittografia** per tutte le evidenze documentali e multimediali fornite in fase di inserimento delle segnalazioni. La segnalazione, inoltrata attraverso la piattaforma web, sarà inviata automaticamente al Gestore della segnalazione, unico destinatario interno per legge a ricevere e gestire la segnalazione.
Qualora il Gestore della segnalazione si trovi in posizione di conflitto di interessi perché la segnalazione riguarda l'OdV, la gestione della segnalazione sarà di competenza dell'Organo Amministrativo e per tale ragione il Gestore della segnalazione dovrà senza indugio trasferirla a mezzo pec all'Organo Amministrativo che attiverà la procedura.
Qualora qualsiasi altro dipendente dell'Azienda riceva una segnalazione, attraverso qualsiasi diverso canale, il ricevente deve cestinare la segnalazione e indicare al segnalante l'utilizzo della piattaforma

per il corretto inoltro della segnalazione al Gestore della segnalazione, presupposto necessario per le garanzie di riservatezza e per accedere al sistema di tutele previste dall'ordinamento. Il dipendente può inviare la segnalazione di condotte illecite, all'ANAC e/o utilizzare un canale di segnalazione pubblico.

CANALE DI SEGNALAZIONE ESTERNO

Il soggetto segnalante può effettuare una segnalazione esterna all'**ANAC** quando:

1. non è prevista, nell'ambito del suo contesto lavorativo, l'attivazione obbligatoria del canale di segnalazione interna o, anche se obbligatorio, non sia attivo o, anche se attivato, non sia conforme;
2. il segnalante ha già effettuato una segnalazione interna e non ha avuto seguito.
3. il segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito o determinerebbe condotte ritorsive;
4. il segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse.

Segnalazione esterna pubblica

La persona segnalante può effettuare una divulgazione pubblica, quando ricorre una delle seguenti condizioni:

1. ha già effettuato una segnalazione interna ed esterna, ovvero ha effettuato direttamente una segnalazione esterna, e non è stato dato riscontro nei termini previsti in merito alle misure previste o adottate per dare seguito alle segnalazioni;
2. ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
3. ha fondato motivo di ritenere che la segnalazione esterna possa comportare il rischio di ritorsioni o possa non avere efficace seguito in ragione delle specifiche circostanze del caso concreto, come quelle in cui possano essere occultate o distrutte prove, oppure in cui vi sia fondato timore che chi ha ricevuto la segnalazione possa essere colluso con l'autore della violazione o coinvolto nella stessa.

Informativa Privacy whistleblowing

L'articolo 13 disciplina la protezione dei dati personali relativi alle segnalazioni, **estendendo le tutele del GDPR e del Codice privacy a tutto il processo di segnalazione**.

Tra gli altri, oltre alle **distinte Informative destinate ai segnalanti e alle persone coinvolte**, l'articolo 13 precisa che **i dati non rilevanti per la segnalazione devono essere immediatamente cancellati**, in conformità con i principi del GDPR che impongono il rispetto dei principi di finalità e minimizzazione del trattamento.

Il decreto richiama anche il **rispetto dei diritti degli interessati**, come definito negli articoli 15 e successivi del GDPR.

Ruoli privacy

Il soggetto che riceve la segnalazione agisce come **titolare del trattamento** ed è tenuto a fornire informazioni specifiche nel rispetto del principio di trasparenza e degli articoli 13 e 14 del GDPR ai segnalanti e alle persone coinvolte.
Inoltre, deve implementare **misure di sicurezza specifiche per garantire la riservatezza** delle informazioni.
La gestione corretta dei soggetti coinvolti nel trattamento è fondamentale per garantire l'accountability richiesta dal GDPR e impone l'obbligo di nominare i soggetti coinvolti nel trattamento in conformità con le disposizioni del GDPR: **autorizzati oppure responsabili del trattamento**, se soggetti esterni all'azienda.

Sicurezza

I titolari del trattamento devono ricevere le segnalazioni e adottare misure tecniche e organizzative adeguate per **ridurre al minimo i rischi** per i diritti e le libertà degli interessati.
Questo processo richiede la **mappatura dei flussi di dati e l'implementazione di misure di sicurezza sia dal punto di vista tecnico (sicurezza informatica e fisica) che organizzativo (procedure e formazione)**.

La valutazione d'impatto – DPIA

L'articolo 13 del Decreto impone ai soggetti destinatari della normativa di adottare misure per proteggere i dati personali dei segnalanti sulla base di una **valutazione d'impatto** (DPIA), come previsto nell'articolo 35 del GDPR.
Nella valutazione d'impatto, è importante **considerare anche i rischi legati ai fornitori coinvolti** (es: **fornitori della piattaforma informatica di segnalazione o gestori delle segnalazioni**) nel processo di segnalazione, in linea con l'articolo 28 del GDPR, che impone una **valutazione preventiva delle garanzie** offerte dai responsabili del trattamento prima di affidare loro l'incarico.

La conservazione dei dati

Per quanto riguarda il periodo di conservazione dei dati, l'articolo 14 del Decreto stabilisce che le segnalazioni, sia interne che esterne, e la relativa documentazione devono essere conservate nel rispetto del principio di limitazione della conservazione, per un *periodo non superiore a 5 anni* a partire dalla data dell'esito finale della procedura di segnalazione.

Mancata o non corretta applicazione del Decreto

Il **segnalante ha il diritto di rivolgersi all'Autorità competente, ANAC**, alle seguenti condizioni:

- se il canale interno obbligatorio **non è attivo oppure è attivo ma non è conforme a quanto previsto** dal Decreto 24 in merito ai soggetti e alle modalità di presentazione delle segnalazioni
- la persona ha già fatto la segnalazione interna **ma non ha avuto seguito**
- la persona segnalante ha fondati motivi di ritenere che se effettuasse una segnalazione interna **alla stessa non sarebbe dato efficace seguito oppure questa potrebbe determinare rischio di ritorsione**
- la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire **un pericolo imminente o palese per il pubblico interesse**.

In caso di violazione della riservatezza o di ostacoli alla segnalazione, l'articolo 21 prevede sanzioni con un **massimo edittale di cinquanta mila euro**.

Firmato digitalmente da:
PANACCIO NICOLA
Data: 19/12/2023 17:41:05