emlex
eva maschietto
massimo maggiore

D.lgs. n. 24 del 10 marzo 2023

(attuazione della direttiva UE 2019/1937 – «Decreto Whistleblowing»)

Uno sguardo ai profili di tutela della *privacy*

Destinatari delle nuove disposizioni (art. 3)

a) Soggetti del settore pubblico

b) Soggetti del settore privato, in particolare:

   i. Imprese che nell'ultimo anno hanno impiegato la media di **almeno 50** lavoratori subordinati (con contratti di lavoro a tempo determinato o indeterminato)

   ii. Imprese operanti in **settori specifici** (servizi, prodotti e mercati finanziari e prevenzione del riciclaggio o del finanziamento del terrorismo, sicurezza dei trasporti e tutela dell'ambiente) **anche se** nell'ultimo anno **non** hanno impiegato la media di almeno 50 dipendenti

   iii. Imprese che adottano il modello organizzativo *ex* **D.lgs. 231/2001**

Da quando si applicano le disposizioni del Decreto *Whistleblowing*

Le disposizioni del decreto troveranno applicazione:

a) A partire dal **15 luglio 2023** (**regola generale**)

I. per i soggetti del settore pubblico
II. per i soggetti del settore privato che, nell'ultimo anno, hanno impiegato una media di lavoratori subordinati superiore a n. 249

b). A partire dal **17 dicembre 2023** (**in via eccezionale**)

I. unicamente per i soggetti del *settore privato* che, nell'ultimo anno, hanno impiegato una media di lavoratori subordinati non superiore a n. 249.

emlex
eva maschietto
massimo maggiore

Whistleblowing e GDPR

La tutela della *privacy* (art. 4)

I soggetti del settore pubblico e del settore privato attivano i propri canali di segnalazione interni garantendo, anche tramite ricorso a sistemi di *crittografia,* la riservatezza

i. dell'identità del segnalante (*whistleblower*)
ii. della persona coinvolta
iii. della persona menzionata nella segnalazione
iv. del contenuto della segnalazione e
v. della relativa documentazione

L'identità del segnalante (*whistleblower*)

a) Non può essere rivelata, in mancanza del suo **consenso espresso**, a persone diverse da quelle autorizzate a ricevere le segnalazioni (art. 12)

b) Va protetta attraverso l'adozione di **sistemi di crittografia**

- Crittografia *end to end* (Garante Privacy, Ord. Ing. 10 giugno 2021, n. 235) ✓

- Registrazione e conservazione dei *log firewall* = identificabilità (Garante Privacy, Ord. Ing. 7 aprile 2022, n. 134) ✗

Adempimenti *privacy* (artt. 13-14 Decreto Whistleblowing)

1) I dati non utili alla segnalazione vanno immediatamente cancellati (principio di minimizzazione – art. 5 GDPR)
2) I dati non possono essere conservati per un periodo superiore a 5 anni dal momento della comunicazione finale della procedura (principio di limitazione della conservazione – art. 5 GDPR)
3) Adozione di misure tecniche e organizzative idonee alla salvaguardia della riservatezza del segnalante, nel rispetto dei principi di *data protection by design and by default* (artt. 25 e 32 GDPR)
4) Conclusione dei contratti con i responsabili del trattamento (es. fornitore sistema informatico del canale di segnalazione, art. 28 GDPR)
5) Nomina referente del titolare del trattamento con apposita autorizzazione al trattamento dei dati del segnalante (art. 29 GDPR)
6) **Informativa privacy *ad hoc*** *(*art. 13 GDPR*)*
7) Eventuale accordo di contitolarità del trattamento dei dati (art. 26 GDPR)
8) Aggiornamento del registro dei trattamenti (art. 30 GDPR)
9) Svolgimento di una valutazione di impatto sulla protezione dei dati (DPIA, art. 35 GDPR)
10) Garantire l'esercizio dei diritti degli interessati nella misura in cui non derivi un pregiudizio effettivo e concreto alla riservatezza del segnalante (art. 2-undecies, lett. f) del Codice Privacy)

Sanzioni (art. 21)

L'ANAC può applicare una sanzione amministrativa pecuniaria

a) da **euro 10.000 a 50.000** quando accerta che:
   i. sono state commesse ritorsioni
   ii. la segnalazione è stata ostacolata/si è tentato di ostacolarla o è stato violato l'obbligo di riservatezza
   iii. non sono stati istituiti canali di segnalazione o non sono state adottate procedure per l'effettuazione e la gestione delle segnalazioni o la loro adozione/implementazione non è conforme alla normativa
   iv. non è stata svolta l'attività di verifica e analisi delle segnalazioni ricevute

b) da **euro 500 a 2.500** quando accerta che:
   i. è stato violato l'obbligo di riservatezza circa l'identità del segnalante

La normativa impone alle piccole aziende che applicano i modelli organizzativi *ex* d.lgs. 231/2001 di prevedere sanzioni disciplinari nei confronti di chi abbia violato l'obbligo di cui alla lettera b) i. (art. 21 comma 2)

Attenzione

Rimane ferma l'applicazione delle sanzioni amministrative pecuniarie ex art. 83 GDPR e l'obbligo di risarcimento dei danni ex art. 82 GDPR.

Contatti

massimo.maggiore@emlex.it
giulio.monga@emlex.it
marco.dicioccio@emlex.it