NT+ Diritto Norme & Tributi Plus | Il Sole 24 ORE

Civile

Data Protection Impact Assessment, gli adempimenti Privacy nel sistema di Whistleblowing

*di Cristina Rabazzi**

26 Maggio 2023

NT+ Contenuto esclusivo Norme & Tributi Plus

Con il **D.Lgs. 24/2023** il legislatore italiano ha recepito la **Direttiva (UE) 2019/1937** , riguardante la protezione delle persone che segnalano illeciti, proteggendole da possibili ritorsioni dirette o indirette. Nel nostro ordinamento, il Whistleblowing era già stato introdotto, nel settore privato, con la Legge 179/2017 e nel settore pubblico con il D.Lgs. 165/2001. Rispetto all'impianto normativo esistente, il recente Decreto ha introdotto delle **novità che impattano in modo rilevante sulla Privacy**. Di seguito alcuni aspetti che meritano particolare attenzione.

➧ ***La riservatezza del whistleblower***: *l'art. 3* fornisce una **accezione di segnalante molto più ampia** di quella preesistente, includendo non solo il dipendente, pubblico e privato, ma anche **tutti i soggetti che sono o sono stati in contatto con l'Ente** (tra cui liberi professionisti, consulenti, fornitori, volontari, azionisti, amministratori).
La normativa è incentrata sul **potenziamento della protezione del segnalante** (*art.12*) al fine di garantire che la sua identità non venga rivelata a soggetti diversi da quelli competenti a ricevere e a dare seguito alle segnalazioni, salvo il suo espresso consenso, sino alla conclusione dei procedimenti che ne sono scaturiti, tenuto conto dei criteri propri di ogni procedimento. Tale **riservatezza viene estesa anche alle persone coinvolte ed ai facilitatori.**

➧ ***I canali di segnalazione***: oltre al canale *interno* (*artt. 4, 5*), viene **introdotto un canale esterno** (*artt. 6, 7, 8*), **assegnato all'Autorità Nazionale Anticorruzione (ANAC)** e viene prescritta l'adozione di misure **tecniche** (come la *crittografia*) ed **organizzative** (con particolare attenzione alle segnalazioni formulate oralmente o per iscritto) che garantiscano la **riservatezza assoluta del segnalante, delle persone coinvolte e del contenuto della segnalazione.** È altresì prevista la possibilità di effettuare una **divulgazione pubblica**, qualora gli altri due canali non prestino le garanzie dovute o quando la violazione possa comportare un pericolo imminente o palese per il pubblico interesse (*art. 15*).

➧ ***La tutela del trattamento dei dati***: in base *all'art. 13*, ogni informazione raccolta in tale processo deve essere trattata in conformità al **Reg. (UE) 2016/679 (GDPR)** , nel rispetto del *più ampio principio di Accountability* (*art. 24 GDPR*) e di quelli di *privacy by design e privacy by default* (*art. 25 GDPR*).
I diritti riconosciuti a tutela dell'interessato (incluso anche il segnalato), di cui agli a*rtt. 15 – 22 GDPR*,

potranno essere esercitati **salvo quando da tale esercizio possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante** (art. 2-undecies D.Lgs. 196/2003).

Gli adempimenti Privacy nel sistema di Whistleblowing

Alla luce di quanto illustrato, qui di seguito si delineano **i principali adempimenti necessari per rendere il sistema di Whistleblowing conforme alla normativa Privacy.**

Nel rispetto della ***privacy by design*** ed ai sensi *dell'art. 13, c. 6*, occorre innanzitutto **predisporre una DPIA (Data Protection Impact Assessment)**, per analizzare i rischi che possono derivare dal trattamento e per adottare un modello di gestione delle segnalazioni, individuando le misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato e disciplinando il rapporto con eventuali fornitori esterni, *ex art. 28 GDPR*.

In relazione a quest'ultimo punto, la **scelta del fornitore**, specie per lo sviluppo del canale di segnalazione, è **particolarmente delicata.** Merita di essere menzionato il **provvedimento del Garante (n. 9768363, 07/04/22)** , con cui ha sanzionato una Azienda Ospedaliera in quanto, tra le diverse irregolarità rilevate, si era avvalsa di una **applicazione web di Whistleblowing, fornita da una software house esterna**, anch'essa sanzionata, basata su sistemi *open source* che, non essendo stati correttamente configurati, **registravano e conservano i dati di navigazione degli utenti**, consentendo l'identificazione di chi la utilizzava, compresi i segnalanti.

È altresì importante fornire una **idonea e preventiva informativa ai lavoratori** in merito al **trattamento dei dati personali effettuato per finalità di segnalazione** (*art. 13, c. 4*), come pure fornire le opportune istruzioni circa il **funzionamento del canale di segnalazione adottato e i presupposti per effettuare una segnalazione** (*art. 5, c. 1, lett.e)*).

Nel rispetto della ***privacy by default*** e del principio di minimizzazione, nella fase di raccolta della segnalazione, devono essere trattati **solo i dati strettamente necessari alla sua gestione**, dovendo procedere alla **cancellazione immediata di quelli raccolti accidentalmente** (art. 13, c. 2).

Il Decreto (*art. 4, c. 4*) prevede la possibilità per determinati Enti di **condividere il medesimo canale di segnalazione.** In tali casi, occorre un **accordo di contitolarità**, ai sensi *dell'art. 26 GDPR*.

Occorre, infine, prestare particolare attenzione alla ***Data Retention*** (*art. 14*). Il legislatore, in ossequio al **principio di limitazione** della conservazione, di cui all'art. 5, par.1, lett. e) GDPR, ha stabilito che le segnalazioni possono essere **conservate solo per il tempo necessario alla loro definizione** e, in ogni caso, per un periodo **non superiore a cinque anni**, a decorrere dalla data di comunicazione dell'esito finale.

_____

**A cura dell'Avv. Cristina Rabazzi, Gebbia Bortolotto Penalisti Associati*