Circolare Adempimenti Whistleblowing

SOMMARIO

WHISTLEBLOWING E PROTEZIONE DATI:

Gli adempimenti per garantire la compliance del trattamento dei dati personali

Il D.Lgs. 24/2023, che ha recepito la Direttiva Whistleblowing, ha introdotto **rilevanti novità** estendendo l'ambito di applicazione ai soggetti privati che hanno impiegato, nell'ultimo anno, una media di ALMENO 50 LAVORATORI subordinati con contratti di lavoro a tempo indeterminato o determinato, o che, a prescindere dal requisito numerico, operano in mercati regolamentati: sicurezza, trasporti, tutela del risparmio, ambiente.

COSA CAMBIA

La "segnalazione" può avvenire, ai sensi di legge, in **forma scritta od orale**: oggetto delle segnalazioni sono violazioni del diritto dell'Unione e del diritto interno intese come "*informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia […] intrattiene un rapporto giuridico* […]".

È, dunque, di fondamentale importanza, per tutti gli operatori che già dispongono di uno strumento per l'acquisizione e la gestione delle segnalazioni di condotte illecite e per coloro che sono tenuti a adottarlo, rivedere il proprio sistema attuale e implementare punti di azione per rendere i propri strumenti conformi agli standard.

Di seguito si fornisce un Vademecum, **con annessa documentazione allegata**, per la verifica degli standard dei processi e dei tool.

LE PROCEDURE

Le procedure devono prevedere un riscontro di ricevimento e presa in carico della segnalazione al segnalante **entro 7 giorni** dal ricevimento della stessa; al segnalante deve essere fornito un follow up entro 90 giorni in relazione all'esito della procedura avviata e deve essere comunicato l'esito finale a chiusura dell'indagine. In caso di segnalazione orale, deve essere acquisito il consenso del segnalante a documentare la segnalazione in forma scritta da parte del personale addetto.

Canale di segnalazione interna

Il canale di segnalazione interna, attivato sentite le organizzazioni sindacali, deve essere progettato con misure tali da garantire la riservatezza dell'identità del segnalante, delle persone coinvolte e comunque menzionate nella segnalazione. La gestione del canale è affidata a una persona o a un ufficio interno dedicato oppure ad un soggetto esterno, anch'esso autonomo. Rimane affidata al RPCT per i soggetti già obbligati alla sua nomina. Le segnalazioni possono assumere FORMA SCRITTA, anche con modalità informatiche, oppure in FORMA ORALE attraverso linee telefoniche o sistemi di messaggistica vocale ma anche, su richiesta del whistleblower, mediante un incontro diretto fissato entro un termine ragionevole.

La segnalazione esterna

Novità assoluta, che lascia autonoma nella valutazione del segnalante di attivare tale percorso al verificarsi di una delle condizioni indicate:

- se nel contesto lavorativo l'attivazione del canale di segnalazione interna non è obbligatoria o il canale non è attivo o non è stato congegnato nel rispetto dei requisiti normativi;
- se il whistleblower ha già fatto una segnalazione interna, ma la stessa non ha avuto seguito o si è conclusa con un provvedimento finale negativo;

- se il whistleblower ha fondato motivo di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito (ad esempio nel caso in cui sia coinvolto nella violazione il responsabile ultimo del suo contesto lavorativo) ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;
- se il whistleblower ha fondato motivo di ritenere che la violazione segnalata possa costituire un pericolo imminente o palese per il pubblico interesse.

L'ANAC è il soggetto che ha l'onere di attivare la piattaforma informatica che consentirà il corretto funzionamento di tale percorso di segnalazione da parte del whistleblower e dovrà offrire le medesime garanzie di riservatezza già indicate per il canale di segnalazione interna.

Le divulgazioni pubbliche

Tale ulteriore modalità di segnalazione (residuale) è lasciata alla discrezionalità del whistleblower, che beneficerà delle medesime misure di protezione per l'utilizzo del canale interno/esterno, solo qualora:

- abbia previamente effettuato una segnalazione interna o esterna senza aver ricevuto riscontro nei termini previsti;
- abbia fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse;
- abbia 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 violazione stessa

Permane, infine, la generale clausola di salvaguardia, in favore delle norme sul segreto professionale degli esercenti la professione giornalistica, con riferimento alla fonte della notizia.

LE INFORMATIVE PRIVACY

I Titolari del trattamento devono fornire le informative sul trattamento dei dati personali, ai sensi degli articoli 13 e 14 del GDPR.

- In allegato **Informativa aggiornata** da rendere definitiva;

REGISTRO DELLE ATTIVITÀ DI TRATTAMENTO

Il Registro della attività di trattamento deve essere **aggiornato** con l'inserimento/aggiornamento dell'attività di whistleblowing quale distinta attività di trattamento condotta dal Titolare.

- Abbiamo provveduto per Vs conto ad aggiornare il **Registro**;

MISURE DI SICUREZZA

Alle procedure e ai sistemi informatici devono essere applicate **MISURE TECNICHE E ORGANIZZATIVE IDONEE** a garantire un livello di sicurezza adeguato al rischio: tra queste NON DEVE ESSERE TRASCURATA la formazione del personale preposto alla gestione delle segnalazioni. I fornitori di sistemi informatici devono rilasciare **specifiche garanzie sulle misure di sicurezza**; deve, inoltre, essere garantita l'idoneità dei sistemi di gestione delle credenziali di autenticazione per gli applicativi mediante autenticazione a multi-fattore; il tracciamento dei log deve essere limitato. Inoltre, le informazioni devono essere scambiate attraverso **protocolli sicuri (HTTPS)**.

- Si allega un **format richiesta informazioni** da trasmettere al Vs fornitore della piattaforma di raccolta delle segnalazioni, da compilare a loro cura e ritrasmettere alla scrivente per l'archiviazione e per allegarlo alla **DPIA finale**;

TEMPO DI CONSERVAZIONE

Il tempo di conservazione della documentazione per trattamento di "Whistleblowing" deve essere individuato nel tempo necessario alla definizione della segnalazione e, comunque, in un tempo **massimo di cinque anni** a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, successivamente al quale deve avvenire la cancellazione.

- Informazione sui tempi di **conservazione aggiornata** ed inserita nel Registro per Vs conto, internamente nella gestione delle segnalazioni va rispettato tale limite;

NOMINE DEGLI AUTORIZZATI AL TRATTAMENTO

La direttiva Whistleblowing richiede espressamente che ogni segnalazione venga indagata dalla "persona o dipartimento più appropriato" al fine di garantire l'indipendenza e l'assenza di conflitto di interessi. Devono, quindi, essere correttamente **individuati i soggetti coinvolti nel Trattamento** in base al ruolo mediante specifiche nomine ad autorizzati al trattamento che prevedano, tra l'altro, il divieto di raccolta dei dati eccedenti e l'obbligo di cancellazione immediata di dati accidentalmente acquisiti. Adeguati **profili di autorizzazione informatica** devono essere contemplati ai fini del divieto di accesso non autorizzato da parte dei membri del personale che non hanno ricevuto la nomina quali autorizzati al trattamento.

- Relativamente alle **Autorizzazioni al trattamento** queste sono state già adottate; verificate e in caso di necessità contattateci e ritrasmetteremo il format da adottare; nel caso in cui il RPCT si avvalga di più soggetti per le gestioni delle segnalazioni, si consiglia di adottare uno specifico ***atto organizzativo*** di individuazione di tali soggetti; Relativamente ai **profili informatici** specificare tale necessita al Vs fornitore;

NOMINA DEI RESPONSABILI (E SUB-RESPONSABILI) DEL TRATTAMENTO EX ART. 28 GDPR

Il rapporto con fornitori esterni che trattano dati per conto Vs, in particolare in questo caso i fornitori di piattaforme informatiche, deve essere puntualmente disciplinato e formalizzato, utilizzando appositi modelli di nomina.

- Abbiamo già trasmesso la documentazione per la designazione dei Responsabili del trattamento, ma alleghiamo **l'atto di designazione**, da ritrasmettere alla scrivente per l'archiviazione e per allegarlo alla **DPIA finale**;

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI - "DPIA"

È OBBLIGATORIO sottoporre il trattamento di gestione delle segnalazioni a **Valutazione d'Impatto (DPIA),** ai sensi dell'art. 35 del GDPR.

- Abbiamo predisposto un format quasi pronto per l'adozione finale, da integrare con le informazioni a noi mancanti ed evidenziate in giallo; una volta terminato si prega di firmarlo e ritrasmetterlo alla scrivente per l'apposizione del parere DPO;

Allegati (da rendere definitivi):

- **Allegato I.W._Informativa Privacy Whistleblowing**: da pubblicare nella sezione privacy del sito web e da rendere disponibile ai Whistleblower;
- **Check list** da richiedere al fornitore/i della piattaforma delle segnalazioni;
- **Atto designazione Responsabile del trattamento ex art. 28**, fornitore/i della piattaforma informatica delle segnalazioni;
- **DPIA 02.01- WHISTLEBLOWING**: da integrare con le informazioni mancanti (evidenziate) in particolare il fornitore della piattaforma delle segnalazioni e le misure di sicurezza che la stessa possiede, firmare-protocollare o adottare atto con numero ufficiale, e ritrasmettere per parere finale DPO.