ADEMPIMENTI IN TERMINI DI TRATTAMENTO DEI DATI PERSONALI

BREVE GUIDA PRATICA

Documento aggiornato il 11 gennaio 2023

I trattamenti di dati personali effettuati dai soggetti obbligati sono considerati necessari per adempiere a un obbligo legale al quale è soggetto il titolare del trattamento (artt. 6, par. 1, lett. c), 9, par. 2, lett. b), e 10 del GDPR).

Il presente documento affronta i seguenti aspetti:

1. nomina di responsabile esterno del trattamento dei dati;
2. pubblicazione dell'informativa sui dati personali;
3. registrazione delle attività di trattamento;
4. analisi dei rischi e misure di sicurezza e Valutazione di impatto sulla protezione dei dati.

1. Nomina di responsabile esterno del trattamento dei dati

Occorre firmare e inviare al soggetto fornitore la nomina di responsabile esterno del trattamento dei dati. Il progetto WhistleblowingPA mette a disposizione una nomina prefirmata, da controfirmare e inviare all'indirizzo gdpr@whistleblowing.it o all'indirizzo PEC wbpa@pec.whistleblowingsolutions.it. Gli enti che hanno già provveduto non devono re-inviarla. La nomina è disponibile al seguente link.

La "catena" di nomine relative alla titolarità e responsabilità dei dati personali nel progetto WhistleblowingPA è spiegata in una specifica FAQ nella pagina di assistenza. Purtroppo, non è possibile da parte nostra accettare nomine personalizzate da parte degli enti che utilizzano la versione standard poiché non saremmo in grado di processare oltre 1.700 documenti diversi per un progetto che mettiamo gratuitamente a disposizione degli enti. D'altra parte, gli enti che adottano una soluzione personalizzata possono proporre un testo maggiormente allineato alle proprie procedure interne.

2. Pubblicazione dell'informativa sui dati personali

Con riguardo al principio di "liceità, correttezza e trasparenza", il Titolare ha l'obbligo di fornire preventivamente a tutta la platea dei possibili soggetti interessati specifiche informazioni sul trattamento dei dati personali e deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 del GDPR.

Un'informativa chiara ed esaustiva ai sensi dell'Art. 13 del GDPR deve essere fornita a tutti i dipendenti e agli altri soggetti che presentano segnalazioni di condotte illecite includendo tale documento informativo nell'atto organizzativo adottato dal Titolare per la gestione delle segnalazioni, o pubblicandolo in un'apposita sezione dell'applicativo informatico utilizzato per l'acquisizione e gestione delle segnalazioni, o, ancora, indicandolo nei contratti individuali di lavoro. Whistleblowing

Solutions e Transparency International Italia raccomandano fortemente la pubblicazione dell'informativa direttamente nella pagina dedicata al whistleblowing.

3. Registrazione delle attività di trattamento

L'art. 30 del GDPR prevede tra gli adempimenti principali del Titolare la tenuta del registro delle attività di trattamento, che deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

A tal fine è importante sottolineare come possano essere trattate anche categorie particolari di dati e dati relativi a condanne penali e reati (artt. 9, par. 1, e 10 del GDPR), eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati riferiti o riferibili al segnalante, al soggetto segnalato o a terzi comunque coinvolti nei fatti segnalati

Il Titolare deve definire il proprio modello di gestione delle segnalazioni in conformità ai principi della "protezione dei dati fin dalla progettazione" (*privacy by design*) e della "protezione per impostazione predefinita" (*privacy by default*) che dovrebbe tenere conto dei seguenti aspetti:

- ridurre al minimo i dati personali limitando la raccolta e la gestione a ciò che è strettamente necessario avendo cura di comprovare che tali informazioni siano sufficienti, pertinenti e non eccessive;
- limitare la trasmissione di documenti elettronici contenenti dati personali allo stretto necessario;
- definire periodi di conservazione dei dati personali limitati nel tempo e appropriati allo scopo;
- verificare che il sistema consenta la cancellazione dei dati personali a scadenza del periodo di conservazione e che il metodo scelto per l'eliminazione sia adeguato.

A tal fine risulta particolarmente importante **inibire il tracciamento degli accessi** al sistema informatico deputato alla raccolta delle segnalazioni, in particolare quando questo è accessibile esclusivamente da postazioni di lavoro attestate alla rete aziendale interna (es. dispositivi quali firewall e web filtering sono in grado di memorizzare in appositi file di log le operazioni di navigazione effettuate, unitamente a dati che consentono di risalire anche indirettamente ai dipendenti o ad altri soggetti che le hanno effettuate).

Nella redazione della procedura interna per la gestione delle segnalazioni oltre a indicare i responsabili della procedura (RPCT, Amministratore di sistema, staff dell'RPCT, eventuale "custode dell'identità"), il *modus operandi* e i tempi di conservazione delle segnalazioni, occorre dedicare un apposito spazio al **passaggio dell'incarico da un RPCT all'altro**. Come indicato dal Garante della Privacy nella recente Ordinanza in merito (n. 9768363), non appena l'RPCT lascia l'incarico, occorre modificare le credenziali di accesso al sistema.

Risulta importante altresì che i soggetti titolari del trattamento dei dati, che dunque accedono al sistema di whistleblowing, siano soggetti ad **attività formative periodiche** circa le tematiche di sicurezza e protezione dei dati personali.

4. Analisi dei rischi e misure di sicurezza e Valutazione di impatto sulla protezione dei dati

Il Titolare è tenuto a rispettare i principi in materia di protezione dei dati (art. 5 del Regolamento) e i dati devono inoltre essere "trattati in maniera da garantire un'adeguata sicurezza" degli stessi, "compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (artt. 5, par. 1, lett. f), del Regolamento). Il Titolare, nell'ambito della necessaria individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame (artt. 24, 25 e 32 del Regolamento), deve in particolare:

- Adottare misure tecniche per il controllo degli accessi, che consentano di limitare l'accesso ai dati personali ai soli soggetti autorizzati dotati di credenziali di autenticazione e di uno specifico profilo di autorizzazione;
- Cifrare i dati personali sia in transito che *at rest* al fine di rendere incomprensibili i dati personali a chi non abbia un'apposita autorizzazione di accesso;
- Determinare tutto ciò che deve essere crittografato (incluso, in via non esaustiva, dischi rigidi, file, dati provenienti da un database o canali di comunicazione);
- Scegliere il tipo di crittografia in base al contesto e ai rischi individuati prediligendo soluzioni di crittografia basate su algoritmi pubblici notoriamente forti;
- Definire misure per garantire la disponibilità e l'integrità delle informazioni e ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- Determinare ciò che deve essere anonimizzato in base al contesto e alla forma in cui vengono memorizzati i dati personali (compresi i campi del database o estratti dai testi);
- Ridurre la possibilità che i dati personali possano essere correlati;
- Definire una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Il trattamento dei dati personali mediante i sistemi di acquisizione gestione delle segnalazioni presenta rischi specifici per i diritti e le libertà degli interessati, considerata anche la particolare delicatezza delle informazioni potenzialmente trattate, la "vulnerabilità" degli interessati nel contesto lavorativo, nonché lo specifico regime di riservatezza dell'identità del segnalante previsto dalla normativa di settore. Come chiarito di recente dal Garante proprio con riferimento ai trattamenti effettuati mediante applicativi per l'acquisizione e gestione delle segnalazioni illecite, il trattamento dei dati personali effettuati in tale ambito presenta rischi specifici per i diritti e le libertà degli interessati e deve dunque essere sottoposto a **valutazione di impatto ex art. 35 GDPR**. Questo in ragione della particolare delicatezza delle informazioni trattate, nonché degli elevati rischi, in termini di possibili effetti ritorsivi e discriminatori, anche indiretti, per il segnalante, la cui identità è protetta da uno specifico regime di garanzia e riservatezza previsto dalla normativa di settore (tanto a livello nazionale quanto a livello europeo, cfr., da ultimo, la direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione).

Il progetto WhistleblowingPA mette a disposizione il seguente documento per facilitare l'ente nella predisposizione della valutazione stessa.