STUDIO PREVITI
LEGALE ASSOCIATO
ROMA - MILANO

Rapporti tra modello 231 e adempimenti privacy: la DPIA in materia di whistleblowing

Avv. Vincenzo Colarocco & Avv. Marta Cogode

Il dipartimento
Compliance, media e tecnologia

CHI SIAMO E COSA FACCIAMO

Offriamo assistenza giudiziale e stragiudiziale, nei settori di privacy, IT, cybersecurity, comunicazione e compliance aziendale.

Operiamo in stretto contatto con tutte le unità aziendali (risk management, marketing, IT, risorse umane, ecc.) per offrire una consulenza strategica finalizzata all'equilibrio tra innovazione, compliance e business aziendale.

Studio legale dell'anno - settore privacy e cyber security
Il Sole 24 Ore ed. 2020, ed. 2022

Finalista "Attualità legislativa dell'anno: privacy"
Top Legal Awards 2019

Migliore Studio dell'anno – settore Data protection & cybersecurity
Leaders League 2022

SP Tech

CHI SIAMO E COSA FACCIAMO

Dalla profonda esperienza maturata dallo Studio Previti nel campo dell'assistenza legale nasce **SP Tech**. L'integrazione e la sinergia tra le due realtà ci permette di offrire alle aziende soluzioni integrate digitali e legali, sviluppando costantemente nuovi strumenti in grado di rispondere alle specifiche esigenze del cliente.

Crediamo nell'implementazione di nuove tecnologie che consentano di guardare al futuro attraverso la creazione di processi legali standardizzabili, frutto dell'interazione tra tecnologia e creatività umana, in grado di incrementare l'efficienza del servizio, sia in termini qualitativi che quantitativi.

Startup più innovativa dell'anno – settore legal tech

LegalTech Inspiration Award 2022

UIA-International Association of Lawyers & LexisNexis

Topic

STUDIO ASSOCIAZIONE PREVITI PROFESSIONALE

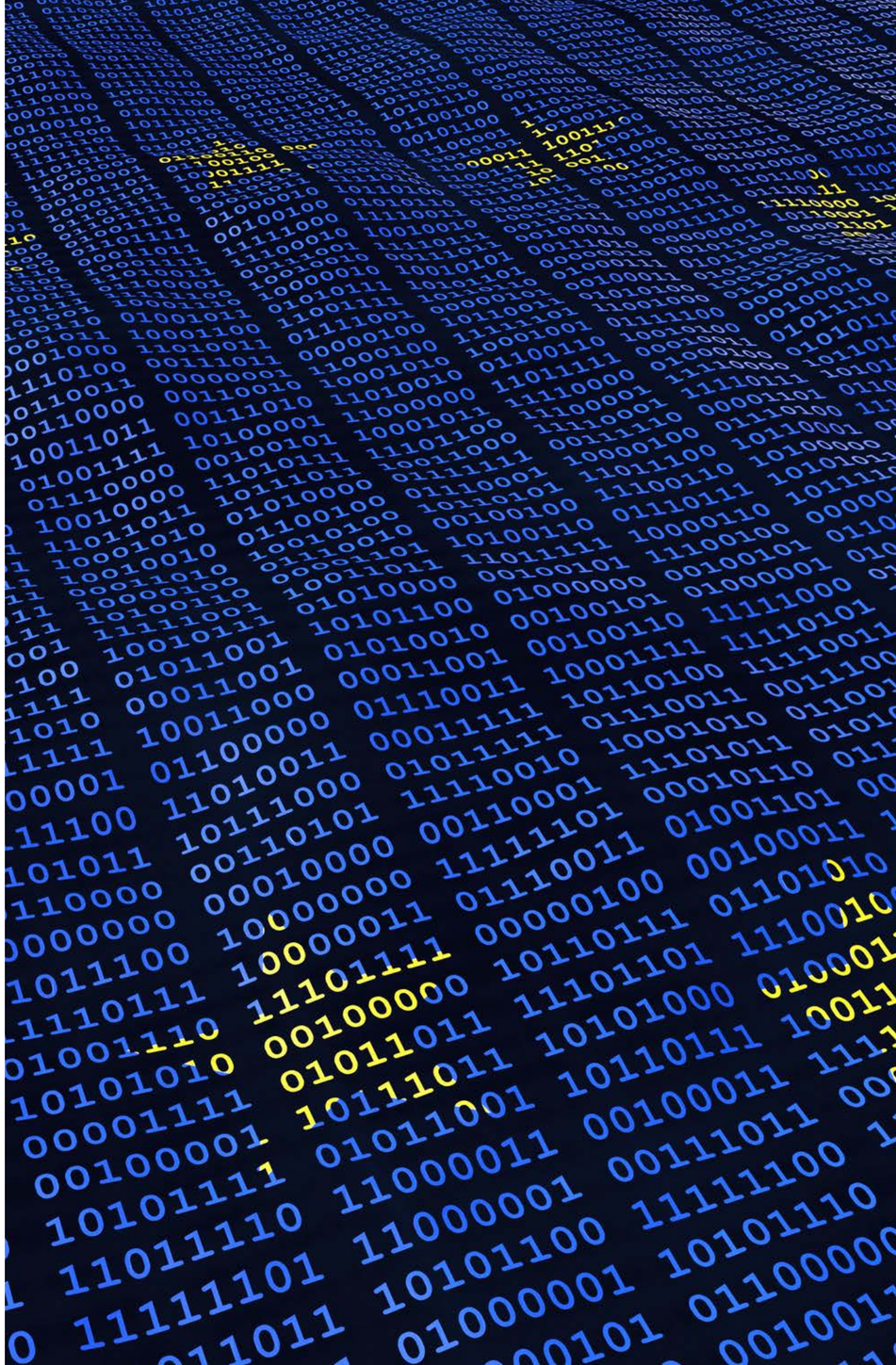
01 Brevi cenni sull'evoluzione della disciplina italiana per la tutela dei segnalatori;

02 Inquadramento generale della normativa in materia di *data protection*;

03 Analisi dei provvedimenti delle Autorità nazionale ed europee sulla DPIA nell'ambito del *whistleblowing*;

04 Focus sulle modalità di conduzione della DPIA.

1. Brevi cenni sull'evoluzione della disciplina italiana per la tutela dei segnalatori



Le tappe principali

L. n. 179/2017 sul whistleblowing in ambito pubblico e privato

L. n. 127/2022 di delegazione europea 2021 per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell’Unione europea

D.Lgs. n. 231/2001 sulla responsabilità amministrativa delle persone giuridiche e degli enti

Direttiva (UE) 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione

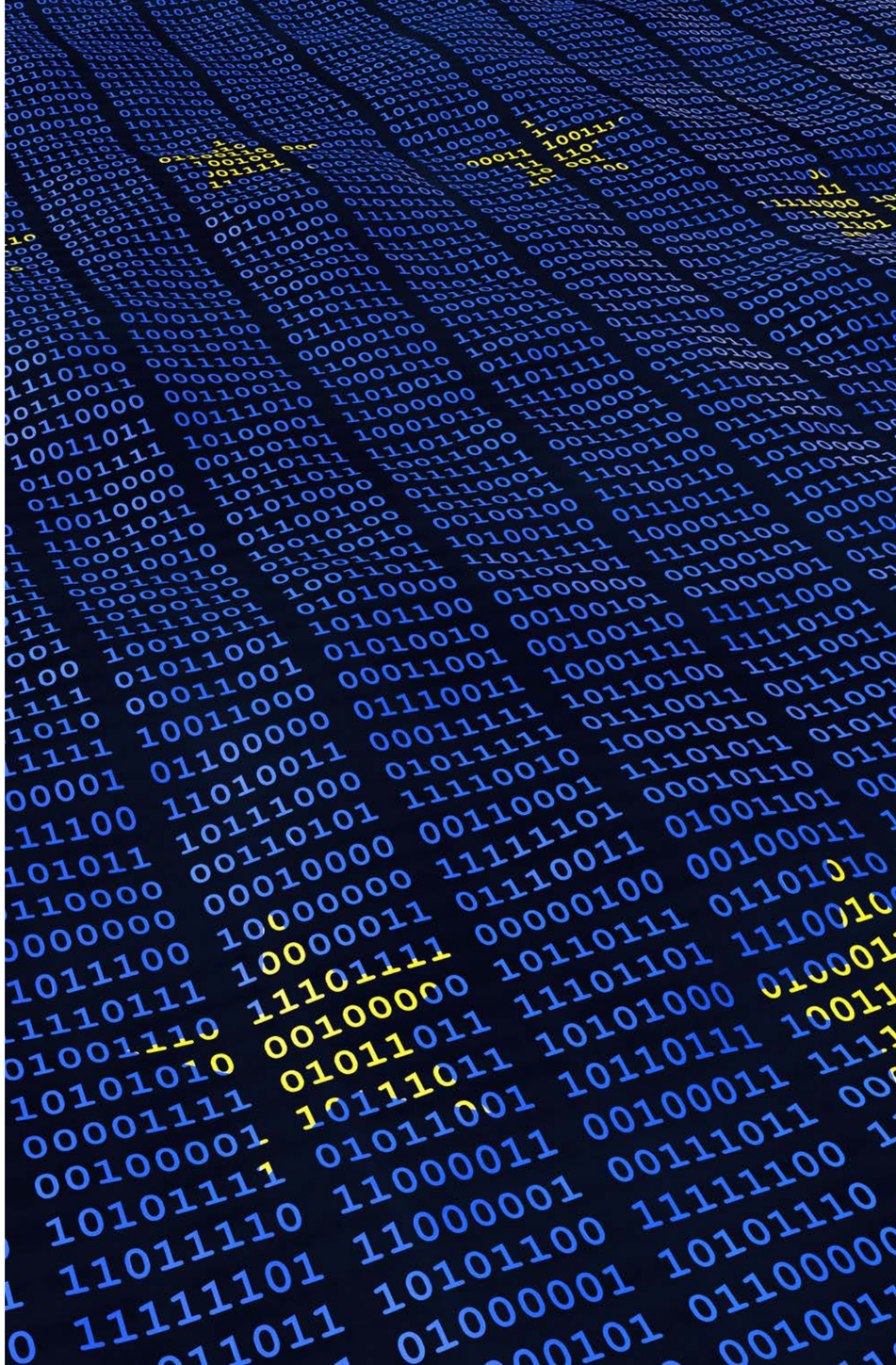
Quali novità con il recepimento della Direttiva?

- Lo scopo della Direttiva è rafforzare l'applicazione del diritto e delle politiche dell'Unione in specifici settori stabilendo norme minime comuni volte a garantire un elevato livello di protezione delle persone che segnalano violazioni del diritto dell'Unione.
- La Direttiva estende l'obbligo di avere un canale interno per le segnalazioni a tutte le aziende con più di 50 dipendenti nel settore privato e a tutti i soggetti nel settore pubblico. Gli Stati membri possono esentare dall'obbligo i comuni con meno di 10 000 abitanti.
- La Direttiva introduce anche l'obbligo di designazione di una persona o di un servizio imparziale competente per dare seguito alle segnalazioni che potrebbe essere la stessa persona o lo stesso servizio che riceve le segnalazioni e che manterrà la comunicazione con la persona segnalante e, se necessario, chiederà ulteriori informazioni e fornirà un riscontro a quest'ultima (cfr. Art. 9 lett.b) della Direttiva e anche ISO 37002:2021 cd. "**Whistleblowing Management Function**").

2. Inquadramento generale della normativa in materia di *data protection*

Quadro normativo:

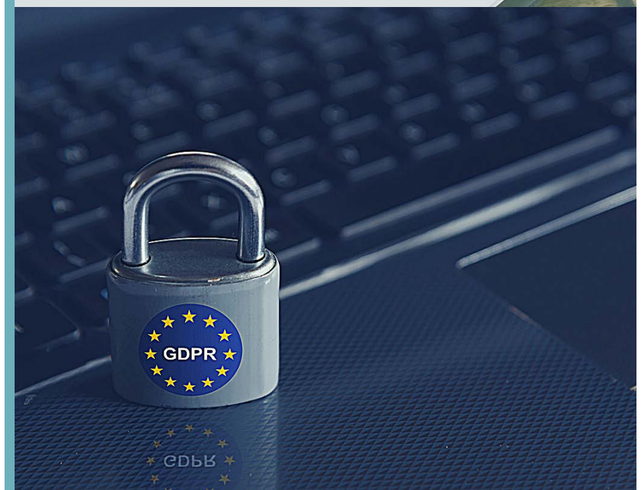
- Regolamento (UE) 2016/679 (“GDPR”)
- Decreto Legislativo n. 196 del 2003 (“Codice Privacy”)



Le sfide principali per la *data protection*

"*Applicare le norme sulla protezione dei dati alle procedure di denuncia implica l'esame dei seguenti aspetti:* ***legittimità dei sistemi di denuncia; applicazione dei principi relativi alla qualità dei dati e di proporzionalità; obbligo di fornire informazioni chiare e complete sulla procedura; diritti del soggetto denunciato; sicurezza dei trattamenti; gestione delle procedure interne di denuncia****; aspetti connessi con il trasferimento internazionale dei dati; obbligo di notificazione e controllo preliminare*" WP29, Parere n. 1/2006.

In premessa: sui principi applicabili e la natura particolare dei dati trattati



1. Il GDPR introduce all'art. 5 i principi generali del trattamento (liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza; responsabilizzazione);
2. Le procedure di whistleblowing prevedono il trattamento di categorie particolari di dati (ai sensi dell'art. 9 del GDPR), oltre a quelli che possono riferirsi a condanne penali e reati (dati giudiziari, ai sensi dell'art. 10 del GDPR).

Privacy by design e *by default*

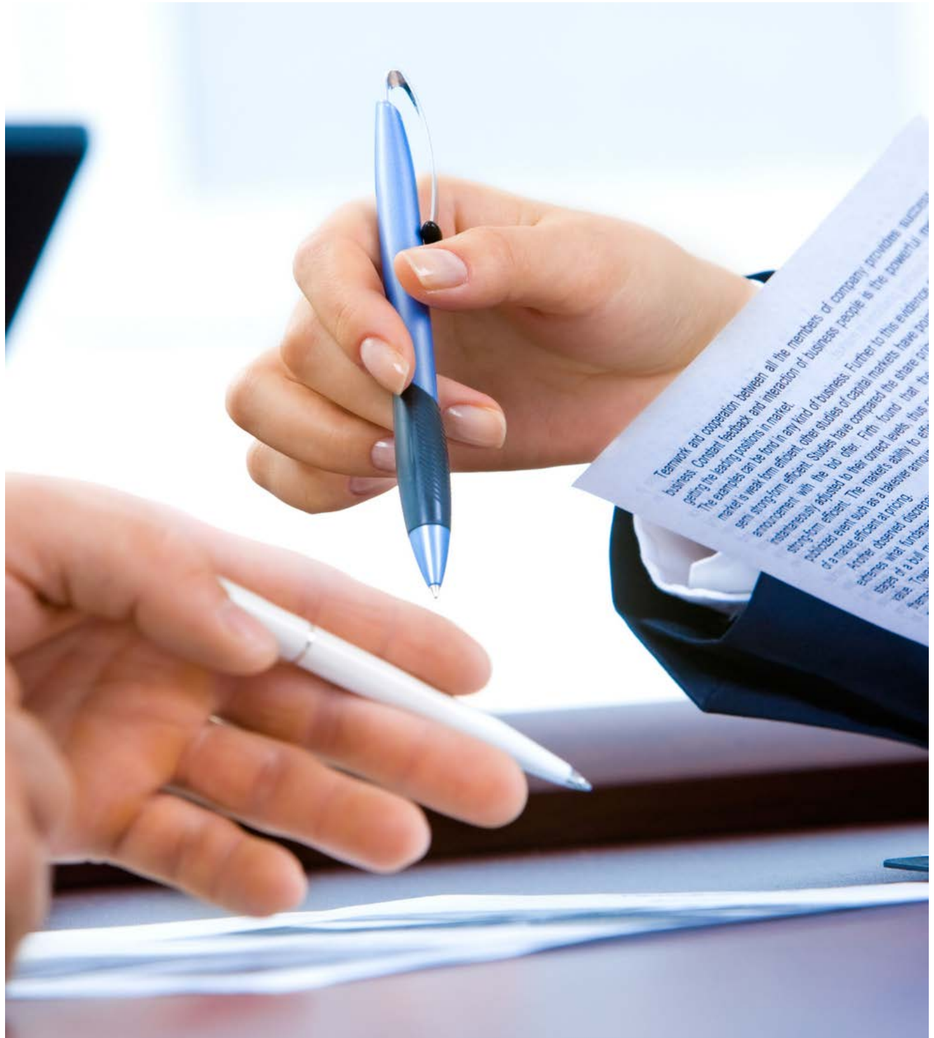
Il GDPR sancisce il principio della *privacy by design*, quindi della "protezione dei dati fin dalla progettazione" (art. 25).

«*Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento* [...] *il titolare del trattamento mette in atto misure tecniche e organizzative adeguate, quali la* ***pseudonimizzazione***[...]»

Rispetto a tali garanzie, il titolare del trattamento deve perciò attenersi alla disciplina sulla protezione dei dati ed assicurare la conformità dell'intera procedura delle segnalazioni di *whistleblowing*.

Il diritto all'informazione (artt. 13-14)

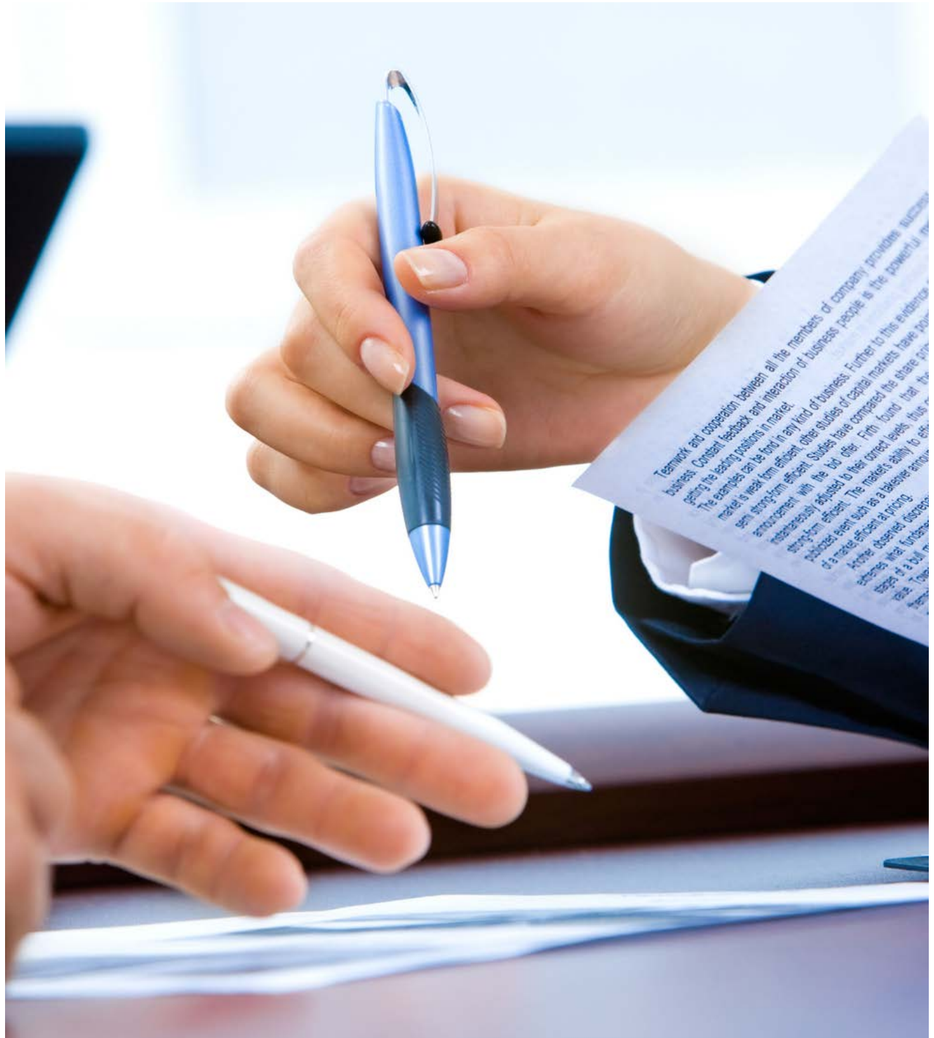
Il titolare ha l'obbligo di fornire agli interessati l'informativa sul trattamento dei dati personali ai sensi degli artt. 13 e 14 del GDPR.
Nell'ambito delle procedure di *whistleblowing* tale informativa (che può essere, ad esempio, inclusa nell'atto organizzativo adottato dall'amministrazione per la gestione delle segnalazioni ovvero pubblicata in un'apposita sezione dell'applicativo informatico utilizzato per l'acquisizione e gestione delle segnalazioni), deve essere resa preventivamente a tutta la platea dei possibili soggetti interessati.



…segue sul diritto all'informazione

La segnalazione resta assoggettata ad obblighi di riservatezza e segretezza, fatta eccezione per i casi in cui:

- l'anonimato non sia opponibile per motivi di indagine giudiziaria;
- sia accertata, anche con sentenza di primo grado, la responsabilità penale del segnalante per i reati di calunnia o diffamazione
- sia accertata, anche con sentenza di primo grado, responsabilità civile dipendente da reato nei casi di dolo o colpa grave



I diritti degli interessati nel Codice Privacy

La normativa nazionale (Codice Privacy, come novellato dal D.Lgs. n. 101/2018) prevede una **specifica disposizione** a tutela della riservatezza dell'identità del segnalante: **l'art. 2-*undecies*, comma 1, lett. f)** prevede che, nell'ambito di una segnalazione whistleblowing, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati, non può esercitare i diritti previsti dagli articoli da 15 a 22 (e in particolare il diritto di accesso) del GDPR poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante.

Ricapitolando: sugli adempimenti del titolare

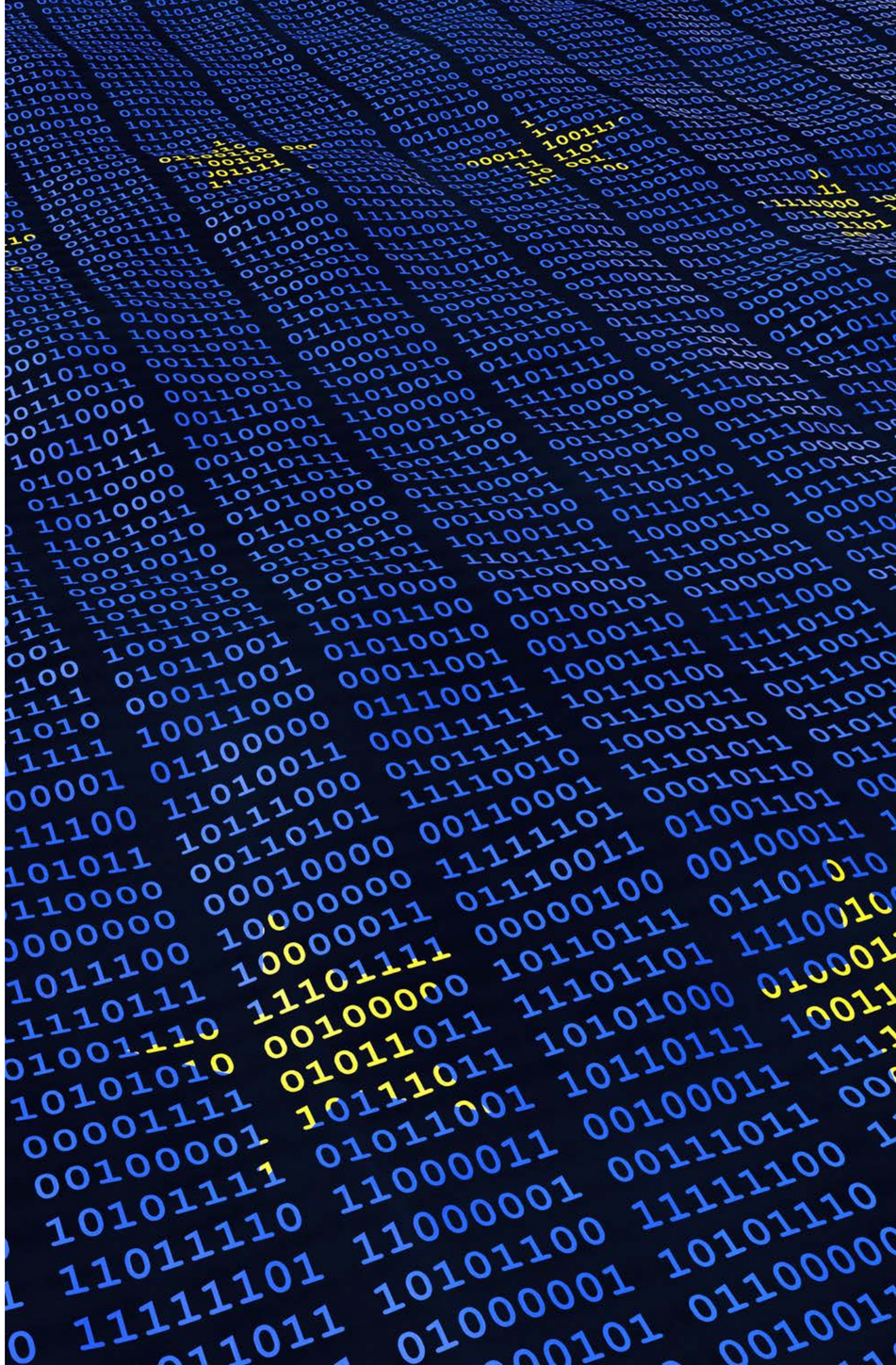
1. Il **fornitore** della piattaforma per il *whistleblowing* deve sempre essere nominato quale **responsabile** del trattamento ai sensi dell'art. 28 del Regolamento (UE) 679/2016 (GDPR).
2. Gli **interessati** (nello specifico il segnalante) devono ricevere idonea **informativa** ai sensi dell'art. 13 GDPR.
3. Il ***whisthleblowing*** deve essere inserito quale **trattamento** specifico all'interno del registro redatto ai sensi dell'art. 30 GDPR.
4. Il titolare deve adottare ogni idonea misura di sicurezza ai sensi dell'art. 32 GDPR;
5. Le segnalazioni devono essere **conservate** per un arco di tempo non superiore al conseguimento delle finalità per cui sono state trattate. L'ANAC, in assenza di un periodo di conservazione indicato dal legislatore o dal Garante privacy, ha individuato tale termine in **10 anni** dal ricevimento della segnalazione, fatte salve differenti esigenze dovute all'instaurazione di un eventuale giudizio (Cfr. *Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001*)

Valutazione d'impatto

È necessario realizzare una valutazione d'impatto sulla protezione dei dati («*Data Protection Impact Assessment* - **DPIA**»), ai sensi dell'art. 35, GDPR) soltanto quando il trattamento «può presentare un rischio elevato per i diritti e le libertà delle persone fisiche». Essa è richiesta in particolare quando il trattamento:

a) sia automatizzato e comporti una valutazione sistematica e globale di aspetti personali relativi a persone fisiche;
b) comporti il trattamento su larga scala di categorie particolari di dati;
c) consista nella sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

3. Analisi dei provvedimenti delle Autorità nazionali ed europee sulla DPIA nell'ambito del whistleblowing



In premessa: le fonti principali nel *Soft Law*

- **Linee guida del WP29** *concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679* (WP 248 del 4 aprile 2017).
- **Linee guida dell'ANAC** *in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis del d.lgs. 165/2001* (c.d. whistleblowing).
- **Parere del Garante Privacy sullo schema delle Linee Guida dell'ANAC** (Provv. 4 dicembre 2019, doc. web n. 9215763).

In particolare: le Linee Guida dell'ANAC

Poiché l'acquisizione e gestione della segnalazione dà luogo al "trattamento" di dati personali è necessario tenere in considerazione le responsabilità e gli adempimenti previsti dalla normativa in materia di protezione dei dati personali, tra cui, adozione, tenuta e aggiornamento di un registro delle attività del trattamento ai sensi dell'art. 30 del Regolamento, ***effettuazione, prima dell'inizio del trattamento, di una valutazione d'impatto sulla protezione dei dati ai sensi degli artt. 35 e 36 del Regolamento****.*

La violazione delle disposizioni che prevedono i principi, i presupposti di liceità del trattamento, nonché delle altre disposizioni che prevedono obblighi e adempimenti in capo al titolare o al responsabile dei dati, può comportare l'adozione di provvedimenti correttivi da parte del Garante per la protezione sui dati personali (art. 58, co. 2, Regolamento) con conseguente applicazione delle sanzioni amministrative (cfr. art. 83 Regolamento e art. 166 e ss. d.lgs. 196 del 2003) nonché rilevare sotto il profilo penale e dar luogo a responsabilità civile (cfr. artt. 82 e 84 Regolamento)

I recenti provvedimenti del Garante Privacy:

Provv. 10 giugno 2021, n. 235, doc. web n. 9685922; e da ultimo Provv. 7 aprile 2022, n. 134, doc. web n. 9768363

Il Garante ha precisato che:

- tenuto conto delle indicazioni fornite anche a livello europeo, 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
- il titolare del trattamento deve eseguire una valutazione dei rischi e accertarsi che siano disattivate le funzioni che non hanno una base giuridica, non sono compatibili con le finalità del trattamento, ovvero si pongono in contrasto con specifiche norme di settore previste dall'ordinamento.

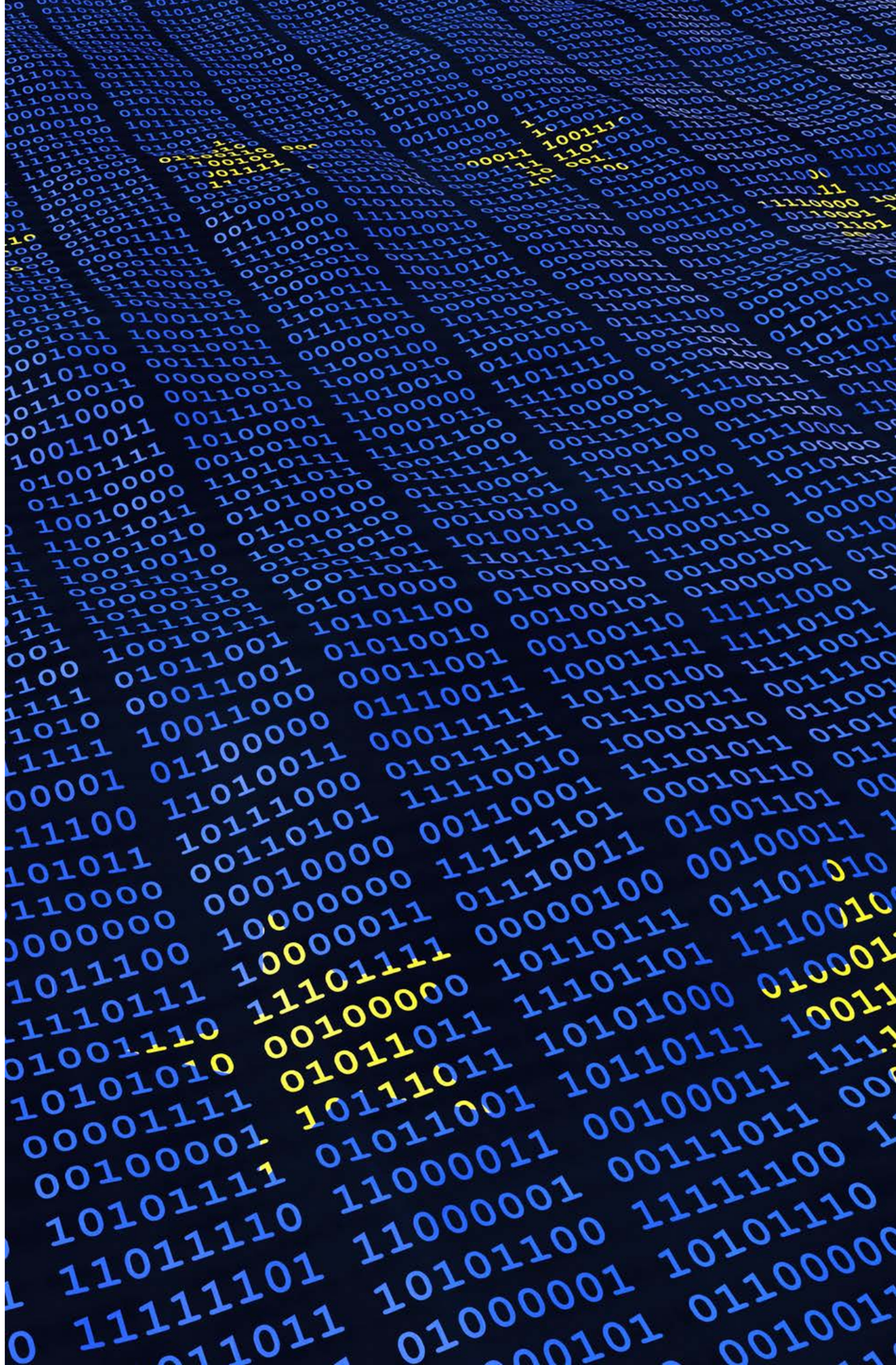
Nei provvedimenti citati, il Garante richiama le Linee Guida dell'ANAC, affermando inoltre che:

- la **crittografia end-to-end** costituisce l'idonea misura tecnica per la conservazione dei dati personali relativi alle segnalazioni.
- nel caso in cui l'acceso dei dipendenti dalle postazioni di lavoro o dispositivi personali connessi alla rete aziendale avvenga tramite "firewall" (la cui configurazione consente il tracciamento dell'indirizzo IP del dispositivo utilizzato per la connessione all'applicativo e username della persona connessa), la registrazione e la conservazione dei **log firewall** e di qualsiasi informazione relativa alla connessione all'applicativo consentirebbe la tracciabilità dei soggetti che lo utilizzano, ivi inclusi, i segnalanti.

La ISO 37002:2021 per la gestione del Whistleblowing

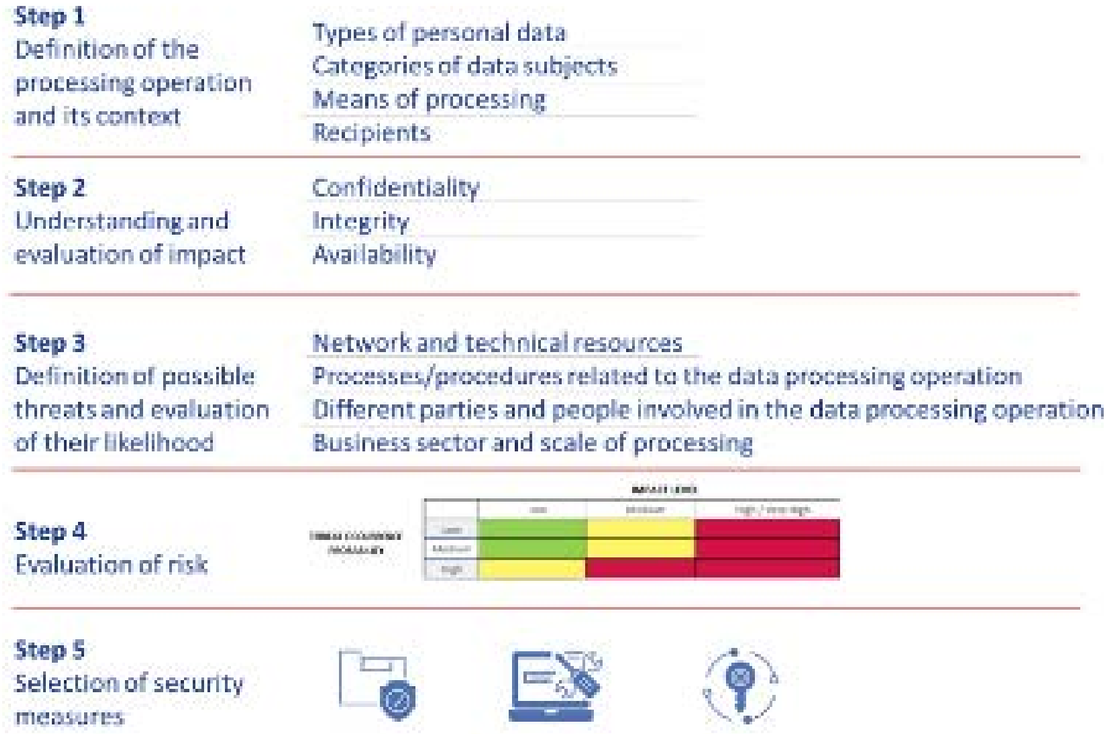
- Ha l'obiettivo di fornire una guida completa per aiutare le organizzazioni a definire, sviluppare, implementare, mantenere efficacemente (per un progressivo miglioramento) un sistema di gestione del *whistleblowing* . Incoraggiare e facilitare la segnalazione di illeciti.
- Conferisce grande importanza al GDPR, in quanto chiarisce la necessità di adottare una valutazione d'impatto nell'ambito della gestione della procedura di *whistleblowing*, poiché tale trattamento può comportare rischi per i diritti e le libertà degli interessati.

4. Focus sulle modalità di conduzione della DPIA



Metodologia nella conduzione della DPIA

La valutazione dei rischi è il primo passo verso l'adozione di adeguate misure di sicurezza per la protezione dei dati personali. L'**European Union Agency for Cybersecurity** (**ENISA**) ha proposto un approccio composto da 5 *step* per supportare le PMI attraverso la valutazione dei rischi rilevanti ai fini di sicurezza e *compliance* con il GDPR.



Contenuto della DPIA

1. una descrizione del trattamento soggetto a DPIA e la relativa finalità, tenendo conto della natura, dell'ambito, del contesto e delle fonti di rischio; nonché una valutazione della necessità e proporzionalità del trattamento;
2. una valutazione dei rischi per i diritti e le libertà degli interessati, in termini di probabilità e gravità degli stessi;
3. le misure previste per affrontare tali rischi, attenuando gli stessi in modo da assicurare la protezione dei dati personali e per dimostrare la conformità al GDPR.

1. Descrizione del trattamento

Art. 35, par. 9, GDPR: necessità di raccogliere le opinioni dei lavoratori o delle organizzazioni sindacali sul trattamento previsto?

Linee Guida del WP29 sulla DPIA

Non sono riportati esempi specifici di quando sia necessario, ma viene precisato che le opinioni possono essere raccolte attraverso vari mezzi, ferma restando la necessità di idonea base giuridica per tale trattamento; qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate e **il titolare del trattamento deve documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati.**

… segue

Dopo aver proceduto con la descrizione della tipologia del trattamento, della categoria di dati e interessati coinvolti, nonché delle finalità e delle basi giuridiche per il trattamento

La DPIA fornisce

1. **Valutazione della necessità e della proporzionalità del trattamento**;
2. **Descrizione delle misure che contribuiscono all'esercizio dei diritti degli interessati;**
3. **Analisi del flusso di dati attraverso il/i singolo/i canale/i delle segnalazioni:** che fornisca una panoramica completa delle modalità con cui vengono raccolte le segnalazioni e delle misure di sicurezza adottate nel corso della procedura (es. attraverso portale *online*/posta/o altro applicativo…);

2. Analisi dei rischi

Il Titolare deve procedere con una valutazione separata degli impatti derivanti dalla perdita di:

01 Riservatezza

02 Integrità

03 Disponibilità

dei dati personali

… segue

L'**ENISA**, ha elaborato un **Tool** che, attraverso una serie di domande di valutazione, mira a sensibilizzare i titolari sul contesto di elaborazione dei dati (che è direttamente rilevante per le minacce). In tale prospettiva, i quesiti da porsi attengono a quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, vale a dire:

1. risorse di rete e tecniche (hardware e software);
2. processi / procedure relativi al trattamento;
3. soggetti coinvolti nel trattamento;
4. settore di attività e portata del trattamento.

Al termine sarà possibile valutare la **probabilità di accadimento per ciascuna minaccia (basso/medio/alto).**

4. Le misure tecniche e organizzative

All’esito della valutazione, il Tool ENISA fornisce un elenco esemplificativo di misure tecniche ed organizzative, che si suggerisce di adottare in funzione del livello di rischio emergente in relazione al trattamento (secondo le categorie già fornite nell’ ISO/IEC 27001 Allegato A e ISO/IEC 27002).

L’ elenco di misure proposto non tiene peraltro conto di altri requisiti di sicurezza specifici del settore, nonché di specifici obblighi normativi, derivanti ad esempio dalla direttiva ePrivacy, dalla direttiva NIS, dalla direttiva sui servizi di pagamento (PSD 2), ecc…

STUDIO PREVITI
LEGALE ASSOCIATO
ROMA - MILANO

Grazie per l'attenzione!

Avv. Vincenzo Colarocco & Avv. Marta Cogode
vincenzocolarocco@previti.it martacogode@previti.it