ODCEC m@ster

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Odcec M@ster La responsabilità amministrativa degli enti ex D. Lgs. 231/2001

I sistemi interni di segnalazione delle violazioni: prassi operative e implementazione del Modello 231 & Whistleblowing: rapporti con la normativa sulla privacy (GDPR)

Dott. Federico Temporiti
Avv. Martina Pesenti

18 novembre 2022

ODCEC m@ster®

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

I sistemi interni di segnalazione delle violazioni: prassi operative e implementazione del Modello 231

Che cos'è il Whistleblowing?

Prevenzione dei rischi e delle situazioni pregiudizievoli per l'organizzazione di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Il **whistleblowing** è uno strumento di derivazione anglosassone attraverso cui **dipendenti pubblici o privati segnalano** potenziali **condotte illecite** commesse da altri soggetti **all'interno del luogo di lavoro**.

Il c.d. «whistleblower» è colui che, nello svolgimento delle sue mansioni, scopre un comportamento illecito e lo segnala internamente all'ente presso cui lavora ovvero alle autorità competenti.

Il «whistleblower» facilita un intervento tempestivo da parte delle autorità competenti, al fine di accertare ed, eventualmente, reprimere quanto segnalato.

Framework Normativo

Internazionale e italiano

- **Convenzione civile sulla corruzione del Consiglio d'Europa del 4 novembre 1999** (ratificata in Italia ad opera della L. 112/2012): prevede la tutela contro «qualsiasi sanzione ingiustificata nei confronti dei dipendenti i quali, in buona fede e sulla base di ragionevoli sospetti, denunciano fatti di corruzione alle persone o autorità responsabili».
- **Convenzione ONU contro la corruzione del 30 ottobre 2003** (Ratificata dalla L. 116/2009): prevede la possibilità di introdurre misure di tutela nell'ordinamento dei singoli Stati a favore di chi segnali - in buona fede e sulla base di «*ragionevoli sospetti*» - eventi concernenti i reati previsti dalla Convenzione.
- **Direttiva 2019/1937**: al fine di armonizzare le normative dei singoli Paesi in materia di whistleblowing, nell'ottobre 2019 è stata emanata la Direttiva 2019/1937 «*riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione*».

- Nel settore pubblico, la **legge n. 190/2012** modifica il **D.Lgs. 165/2001** introducendo l'art. 54-bis («*tutela del dipendente pubblico che segnala illeciti*»). La tutela prevista dal decreto, originariamente estesa solo ai «*dipendenti pubblici*», è stata successivamente ampliata dalla **Legge 179/2017**.
- Nel settore privato, la **Legge 179/2017** modifica il **D.Lgs. 231/2001** aggiungendo all'art. 6 i commi 2-bis e 2-quater.
- La **Legge n. 53/2021** (legge di delegazione europea 2019-2020) stabilisce i principi e criteri che dovranno essere osservati dal Governo italiano nel dare attuazione alla Direttiva 2019/1937.

  Il Parlamento ha rinnovato la delega stessa con la **Legge n. 127 del 4 agosto 2022** denominata "Delega al Governo per il recepimento delle direttive europee e l'attuazione di altri atti normativi dell'Unione europea – Legge di delegazione europea 2021".

Direttiva Ue 2019/1937: le novità

Gli Stati avranno il compito di istituire canali di segnalazione interna ed esterna ampliando anche il novero dei soggetti che possono segnalare (e.g. dipendenti pubblici, azionisti, membri dell'organo di amministrazione, direzione e vigilanza, tirocinanti, qualsiasi persona che lavora sotto la supervisione degli appaltatori etc.)

Obbligo di garantire la riservatezza del whistleblower con trattamento dei dati in conformità al GDPR

Divieto di misure ritorsive e inversione dell'onere della prova

Previsione di sanzioni per garantire la riservatezza del segnalante

Non ci sarà differenza tra settore pubblico e privato

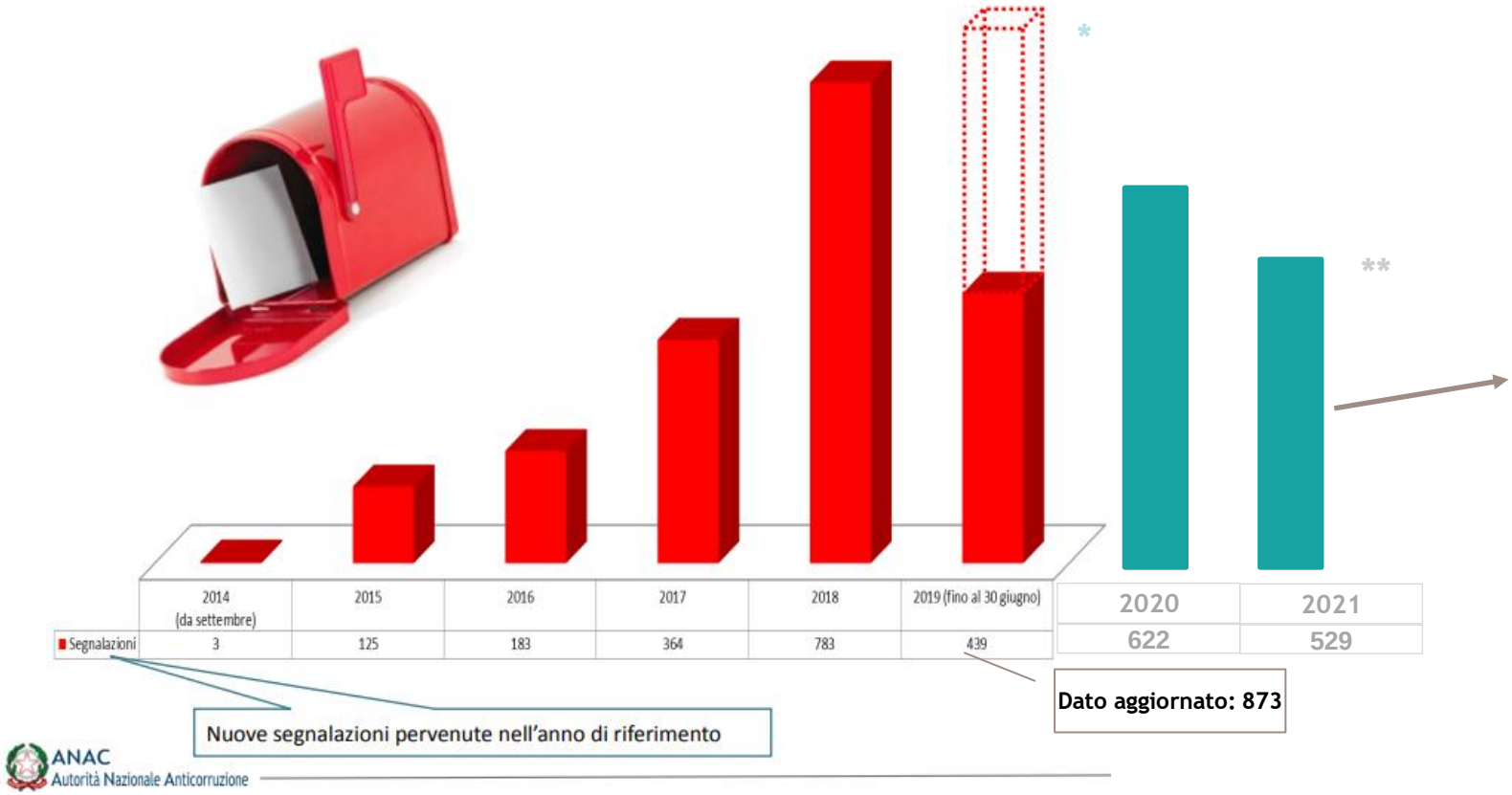
Normativa nazionale e Direttiva UE: le differenze principali

	Legge 179/2017 (art. 6 D.Lgs. 231/2001)	Direttiva (UE) 2019/1937
AMBITO DI APPLICAZIONE	La normativa italiana si applica, nel settore privato, solo agli enti che hanno adottato il Modello di organizzazione e gestione.	La Direttiva si applica indistintamente al settore pubblico e privato e riguarda tutte le imprese con almeno 50 dipendenti, a prescindere dall'adozione del Modello di organizzazione e gestione, nonché ai soggetti operanti nei servizi finanziari e a rischio riciclaggio/finanziamento del terrorismo, indipendentemente dalle dimensioni. In base a un appropriato risk assessment, gli Stati membri possono decidere di applicare la Direttiva anche a soggetti con meno di 50 dipendenti.
VIOLAZIONI	La tutela del segnalante prevista dalla normativa si applica a tutti i casi di condotte illecite rilevanti ai fini dei reati presupposto ex D.Lgs. 231/2001 e violazioni del Modello di organizzazione e gestione.	La Direttiva considera tutte le violazioni relative ad alcuni specifici settori del diritto dell'Unione, tra i quali rientrano appalti, servizi finanziari, sicurezza dei prodotti e dei trasporti, tutela dell'ambiente e dei consumatori.
SEGNALANTI	Quanto alla categoria dei segnalanti, sono tutelati i destinatari del Modello di organizzazione e gestione, quindi dipendenti, amministratori e terze parti.	la Direttiva considera segnalatori coloro che hanno acquisito informazioni sulle violazioni in un contesto lavorativo. Sono quindi tutelati, tra gli altri: gli azionisti delle società, i collaboratori, i dipendenti, i soggetti che assistono i whistleblower, gli ex dipendenti e coloro che hanno conosciuto gli illeciti in fase di selezione o negoziazione precontrattuale.
OBBLIGHI DEGLI ENTI	Agli enti è richiesto di adottare uno o più canali (dei quali ameno uno in forma informatica) che consentano le segnalazioni garantendo la riservatezza dell'identità del segnalante. Quando il soggetto ricevente la segnalazione acquisisce la segnalazione, in base alla Legge deve svolgere l'attività ritenuta necessaria, senza particolari regole.	Gli enti dovranno adottare tre canali di segnalazione (interno, esterno, pubblico). Quanto agli aspetti procedurali, dovranno: a) individuare un soggetto - interno o esterno - per la gestione e l'analisi delle segnalazioni nonché un soggetto che si occupi di seguire le indagini e mantenere la comunicazione con il segnalante; b) consentire al whistleblower di effettuare segnalazioni per iscritto e di trasmetterle per posta (cassetta per reclami o on-line) o di segnalare oralmente (mediante linea telefonica gratuita e/o messaggistica vocale) e, su richiesta, anche di persona; c) comunicare la ricezione della segnalazione entro 7 giorni (le segnalazioni scritte, orali, incluso via telefono e messaggio vocale, o di persona); d) prendere in carico le segnalazioni e mantenere il whistleblower informato, comunicando l'esito entro un tempo ragionevole (non oltre 3 mesi); d) conservare traccia e archiviare le segnalazioni e i relativi follow up; f) fornire informazioni chiare e dettagliate sulle procedure di segnalazione interna.
DIVIETI	E' sancito il divieto di atti di ritorsione o discriminatori nei confronti del whistleblower, per motivi collegati, direttamente o indirettamente, alla segnalazione. Inoltre, sono nulli il licenziamento ritorsivo o discriminatorio del segnalante, nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei suoi confronti.	È vietata qualsiasi forma di ritorsione, comprese le minacce e i tentativi di ritorsione quale, per esempio, il licenziamento, l'imposizione di misure disciplinari, l'inserimento in liste nere, l'annullamento di licenze o permessi, i danni, anche alla reputazione della persona, in particolare sui social media o la sottoposizione ad accertamenti psichiatrici o medici. Sono, altresì, vietate le ritorsioni indiretti che possono essere intraprese contro il soggetto giuridico di cui il segnalante sia proprietario, per cui lavori o a cui sia altrimenti connesso in un contesto lavorativo.

Whistleblowing: alcune domande rilevanti

- **Cosa si intende per canale di segnalazione?**
- **Quanti canali bisogna predisporre?**
- **Il canale deve essere anonimo o no?**
- **Come tutelare la riservatezza?**
- **A quale funzione attribuire la responsabilità?**
- **E' auspicabile nominare un responsabile alternativo?**
- **E' possibile l'outsourcing nella fase di ricezione e validazione della segnalazione?**
- **Le regole previste dalla Direttiva quando saranno vincolanti?**

Whistleblowing: i dati dell'Anac*



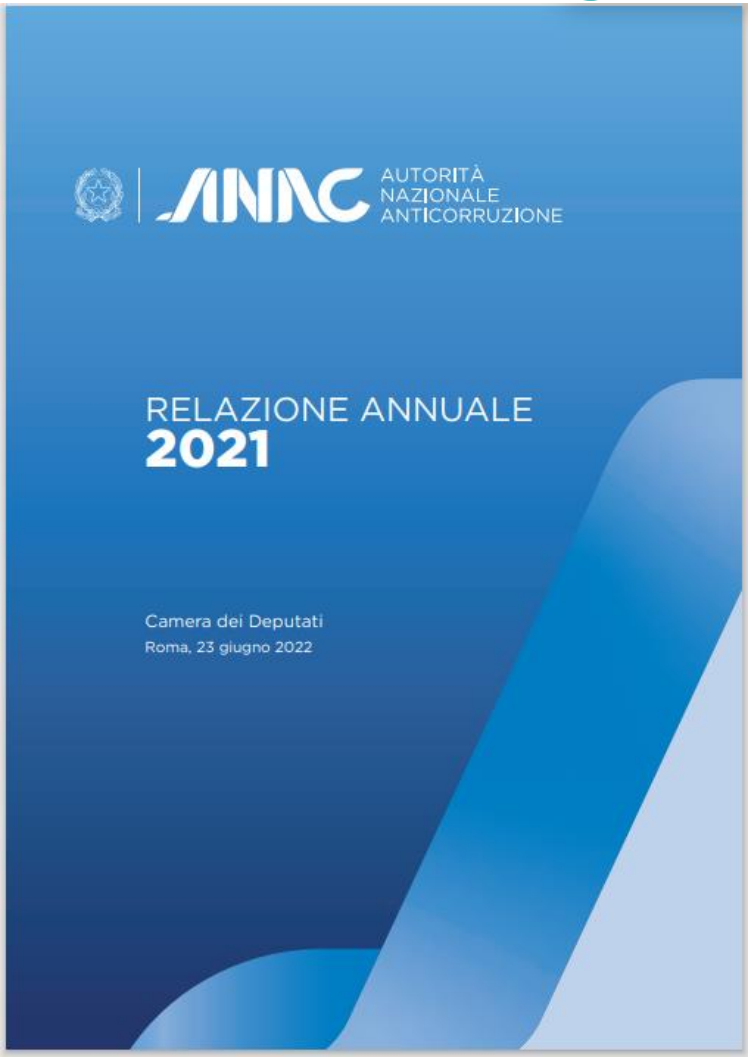
Le segnalazioni si sono ridotte per due ordini di ragioni:

1) **Migliore conoscenza dell'istituto** che ha determinato la segnalazione di fatti riconducibili alla nozione di "condotta illecita" e che quindi le segnalazioni fossero maggiormente rispondenti al dettato normativo;

2) Lo **smart working** ha ridotto il tempo di permanenza in ufficio e anche quindi la segnalazione di irregolarità, illeciti e anomalie. Inoltre, il ruolo degli Rpct all'interno delle amministrazioni si è rafforzato, con la conseguenza che a differenza di qualche anno fa, oggi i dipendenti pubblici segnalano anche all'interno.

***: https://www.anticorruzione.it/-/presentazione-del-4%C2%B0-rapporto-annuale-sul-whistleblowing?redirect=%2Fappuntamenti**
****: https://www.anticorruzione.it/documents/91439/39459199/12.ANAC+-+Relazione+annuale+2022+-+Whistleblowing.pdf/93853064-262f-5eb5-a26d-9d4d8e27dcfe?t=1655914271723#:~:text=www.anticorruzione.it-,Nel%202021%20Anac%20ha%20aperto%20513%20fascicoli%20per%20presunti%20casi,per%20il%20tramite%20della%20piattaforma.**

Whistleblowing: i dati dell'Anac*



Anche a causa dell'emergenza pandemica conseguente alla diffusione del Covid-19, si è registrato un arresto dell'andamento esponenziale delle segnalazioni iniziato nel 2014 e proseguito fino al 2019: il numero delle segnalazioni di illeciti e delle comunicazioni di misure ritorsive pervenute ad ANAC nel corso dell'anno 2021 è stato pari a 529, con una riduzione del 14,95% rispetto all'anno precedente.

Le irregolarità segnalate hanno riguardato soprattutto l'ambito degli appalti pubblici, quello dei concorsi, la gestione delle risorse pubbliche, la mancata attuazione della disciplina anticorruzione, nonché numerosi casi di maladministration, con ricadute penali ogniqualvolta detti casi si sono tradotti in fattispecie criminose, quali, ad esempio, l'abuso d'ufficio.

*: https://www.anticorruzione.it/-/relazione-annuale-di-anac-al-parlamento-in-diretta-dalla-camera-oggi-23-giugno#p6

Whistleblowing e D.Lgs 231/2001: gli impatti della L. 30 novembre 2017 n.179

All'art. 6 d.lgs. n. 231/2001 dopo il comma 2 sono inseriti 3 nuovi commi

2 bis → Prevede significative modifiche ai modelli di organizzazione, gestione e controllo

2 ter → Prevede la possibilità di denunciare l'adozione di misure discriminatorie all'Ispettorato Nazionale del Lavoro.

2 quater → Sancisce la nullità del licenziamento e di ogni altra misura ritorsiva o discriminatoria adottata nei confronti del whistleblower. Disciplina l'onere della prova.

Whistleblowing e D.Lgs 231/2001: gli impatti della L. 30 novembre 2017 n.179

Comma 2 *bis*

I modelli di organizzazione e gestione prevedono:

a) **uno o più canali che consentano ai soggetti indicati nell'articolo 5, comma 1, lettere a) e b), di presentare, a tutela dell'integrità dell'ente, segnalazioni circostanziate di condotte illecite, rilevanti** ai sensi del presente decreto e fondate su elementi di fatto precisi e concordanti, o di violazioni del modello di organizzazione e gestione dell'ente, di cui siano venuti a conoscenza in ragione delle funzioni svolte; **tali canali garantiscono la riservatezza dell'identità del segnalante nelle attività di gestione della segnalazione;**

b) **almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante;**

c) **il divieto di atti di ritorsione o discriminatori, diretti o indiretti**, nei confronti del segnalante per motivi collegati, direttamente o indirettamente, alla segnalazione;

d) nel sistema disciplinare adottato ai sensi del comma 2, lettera e), **sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.**

Art. 5, comma 1 a) da persone che rivestono funzioni di rappresentanza, di amministrazione o di direzione dell'ente o di una sua unita' organizzativa dotata di autonomia finanziaria e funzionale nonche' da persone che esercitano, anche di fatto, la gestione e il controllo dello stesso; b) da persone sottoposte alla direzione o alla vigilanza di uno dei soggetti di cui alla lettera a).

Whistleblowing e D.Lgs 231/2001: gli impatti della L. 30 novembre 2017 n.179

Comma 2 *ter*

I modelli di organizzazione e gestione prevedono che:

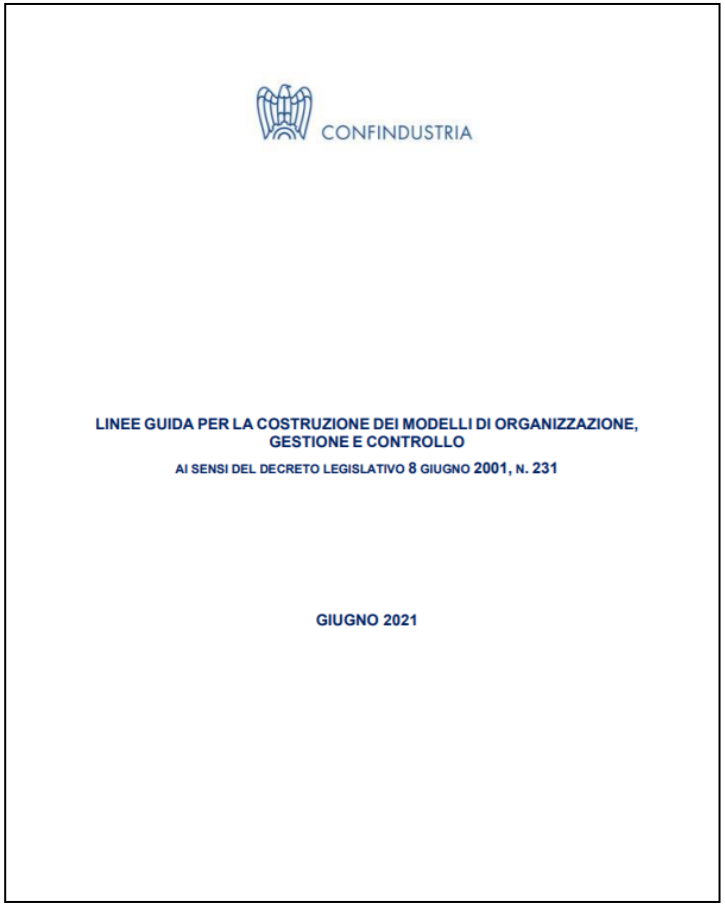
L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis **può essere denunciata all'Ispettorato nazionale del lavoro**, per i provvedimenti di propria competenza, oltre che dal segnalante, anche dall'organizzazione sindacale indicata dal medesimo.

Comma 2 *quater*

I modelli di organizzazione e gestione prevedono che:

Il licenziamento ritorsivo o discriminatorio del soggetto segnalante è nullo. **Sono altresì nulli il mutamento di mansioni** ai sensi dell'articolo 2103 del codice civile, **nonché qualsiasi altra misura ritorsiva o discriminatoria adottata nei confronti del segnalante.** E' onere del datore di lavoro, in caso di controversie legate all'irrogazione di sanzioni disciplinari, o a demansionamenti, licenziamenti, trasferimenti, o sottoposizione del segnalante ad altra misura organizzativa avente effetti negativi, diretti o indiretti, sulle condizioni di lavoro, successivi alla presentazione della segnalazione, dimostrare che tali misure sono fondate su ragioni estranee alla segnalazione stessa.

Whistleblowing e D.Lgs 231/2001: le linee guida di Confindustria


CONFINDUSTRIA

LINEE GUIDA PER LA COSTRUZIONE DEI MODELLI DI ORGANIZZAZIONE, GESTIONE E CONTROLLO

AI SENSI DEL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

GIUGNO 2021

Le imprese dotate del modello organizzativo 231 devono disciplinare le modalità per effettuare le segnalazioni e le modalità di gestione delle stesse, distinguendo fasi e responsabilità, eventualmente **con una procedura ad hoc**

Per quanto riguarda i profili più operativi, la legge prevede che i canali destinati a veicolare le segnalazioni garantiscano la riservatezza dell'identità del denunciante nelle diverse fasi di gestione della denuncia e che, almeno uno di essi, provveda a tali garanzie **con modalità informatiche.**

È quindi fondamentale **che la definizione della policy in materia di whistleblowing proceda di pari passo con la predisposizione degli strumenti informatici di supporto.**

Per dare attuazione alle nuove previsioni si ritiene **che il modello organizzativo debba indicare il "destinatario" delle segnalazioni,** vale a dire il soggetto, l'organo ovvero la funzione incaricati di ricevere e gestire le segnalazioni oggetto della nuova disciplina.

Whistleblowing e D.Lgs 231/2001: il destinatario delle segnalazioni

- L'Organismo di Vigilanza ovvero un altro soggetto, comitato, struttura specificamente individuato;
- Un ente o soggetto esterno dotato di comprovata professionalità, che si occupi di gestire la prima fase di ricezione delle segnalazioni in coordinamento con l'ente;
- Un comitato rappresentato da soggetti appartenenti a varie funzioni (ad esempio legale, internal audit, compliance, HR);
- Il responsabile della funzione compliance;
- Il datore di lavoro nelle PMI.
- RPCT nelle amministrazioni (cfr. Linee Guida Anac)

CON PARTICOLARE RIGUARDO ALL'ODV

E' importante in ogni caso definire anche il ruolo dell'Organismo di Vigilanza. Infatti, il sistema di gestione del whistleblowing rappresenta una parte del più ampio modello organizzativo di cui l'Organismo di Vigilanza è tenuto a monitorare il funzionamento.

Se l'Organismo di Vigilanza non viene individuato come destinatario esclusivo, sembra comunque opportuno coinvolgerlo in via concorrente ovvero successiva, per evitare il rischio che il flusso di informazioni generato dal meccanismo di whistleblowing sfugga del tutto al suo monitoraggio.

Se l'impresa attiva dei canali anche per la segnalazione di illeciti diversi rispetto a quelli considerai dalla legge n. 179 e connessi alla disciplina 231, **si può assegnare al destinatario anche una funzione di filtro: effettuare una prima valutazione sommaria delle segnalazioni** per verificarne l'eventuale rilevanza sul piano 231 e, in caso positivo, informare tempestivamente l'Organismo di Vigilanza

Whistleblowing e D.Lgs 231/2001: le linee guida del Consiglio Nazionale dei Dottori Commercialisti

Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

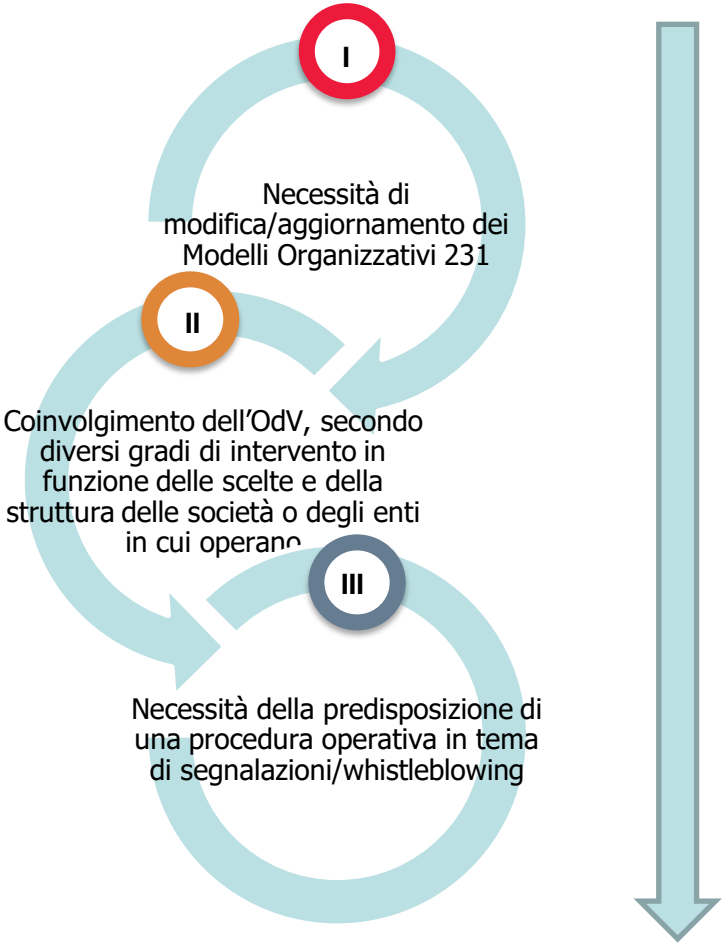
Fondazione Nazionale dei Commercialisti

Documento

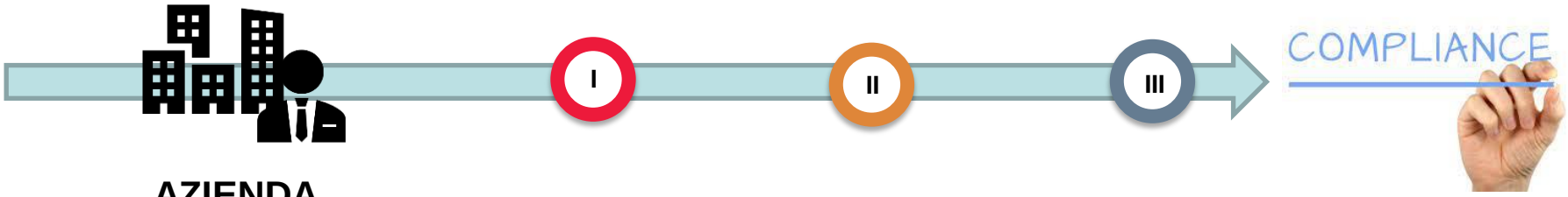
La disciplina del *whistleblowing*: indicazioni e spunti operativi per i professionisti

FNC

12 FEBBRAIO 2021



Whistleblowing e D.Lgs 231/2001: best practice



AZIENDA

I

MOG

- previsione di una sezione descrittiva della L. 179/2017 e ss.mm.ii.;
- indicazione dei canali di segnalazione;
- espressa introduzione del divieto di atti di ritorsione;
- introduzione di sanzioni disciplinari connesse alla violazione del divieto di cui al punto precedente.

II

ODV

- vigilare sull'attività di modifica/aggiornamento del Modello 231;
- verificare l'adeguatezza dei canali informativi;
- gestire – per quanto di competenza – il processo di analisi e valutazione della segnalazione;
- sovrintendere alla formazione dei dipendenti.

III

Procedura WB

- scopo e finalità della procedura;
- normativa di riferimento;
- destinatari della procedura;
- oggetto e contenuto della segnalazione;
- destinatari della segnalazione;
- canali di comunicazione/invio della segnalazione;
- modalità di gestione e verifica della fondatezza delle segnalazioni;
- protezione dei dati e archiviazione/conservazione dei documenti;
- forme di tutela e responsabilità del whistleblower.

Whistleblowing e D.Lgs 231/2001: la tutela del segnalante, del segnalato e……

SEGNALANTE

Il **divieto di atti di ritorsione o discriminatori**, diretti o indiretti, nei confronti del segnalante

Sanzioni nei confronti di chi viola le misure di tutela del segnalante

L'adozione di misure discriminatorie nei confronti dei soggetti che effettuano le segnalazioni di cui al comma 2-bis può essere **denunciata all'Ispettorato nazionale del lavoro**

Le nullità di cui al comma 2 quater **e l'inversione dell'onere della prova**

Tutele previste in materia di rilevazione di informazioni coperte dal segreto d'ufficio, professionale etc previsti ex art. 3 Legge 179/2017

SEGNALATO E IMPRESA

L'inversione dell'onere della prova deve ricevere un'interpretazione di stretto diritto nel senso che, per considerare legittima la sanzione irrogata, deve ritenersi sufficiente la prova della sussistenza – oltre che del comportamento contestato – di un nesso causale tra la sanzione stessa e il comportamento contestato, senza ulteriori accertamenti in ordine alla motivazione del provvedimento adottato (cfr. linee guida Confindustria 2018 –whistleblowing).

Segnalazioni circostanziate di condotte illecite, **rilevanti** ai sensi del presente decreto **e fondate su elementi di fatto precisi e concordanti**. ***No rumors***

Sanzioni di chi effettua con dolo o colpa grave segnalazioni che si rivelano infondate.

Le tutele del segnalante nel settore pubblico (cfr. art. 54 D. lgs. 30 marzo 2001, n. 165) non sono garantite nei casi in cui sia accertata, anche con sentenza di primo grado**, la responsabilità penale del segnalante per i reati di calunnia o diffamazione** o comunque per reati commessi con la denuncia di cui al comma 1 ovvero **la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave**

Whistleblowing e D.Lgs 231/2001: sinergie con altre normative

DISCIPLINA BANCARIA

Per ciò che concerne il settore bancario e finanziario, dal punto di vista normativo merita di essere richiamato il D.Lgs. 72/2015 (di recepimento della Direttiva 2013/36 – c.d. CRD IV) che ha introdotto nel corpo del TUB e del TUF, rispettivamente, gli artt. 52-bis e 4-undecies

Dispositivo dell'art. 52 bis Testo unico bancario

1. Le banche e le relative capogruppo adottano procedure specifiche per la segnalazione al proprio interno da parte del personale di atti o fatti che possano costituire una violazione delle norme disciplinanti l'attività bancaria.
2. Le procedure di cui al comma 1 sono idonee a:
   a) **garantire la riservatezza** dei dati personali del segnalante e del presunto responsabile della violazione, ferme restando le regole che disciplinano le indagini o i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto della segnalazione;
   b) **tutelare adeguatamente il soggetto segnalante** contro condotte ritorsive, discriminatorie o comunque sleali conseguenti la segnalazione;
   c) **assicurare per la segnalazione un canale specifico, indipendente e autonomo.**
3. La presentazione di una segnalazione non costituisce di per sé violazione degli obblighi derivanti dal rapporto di lavoro

Whistleblowing e D.Lgs 231/2001: sinergie con altre normative

DISCIPLINA BANCARIA

Sul tema, in base alla delega ricevuta dalla norma primaria, la Banca d'Italia è intervenuta anche in via regolamentare, aggiornando la Circolare n. 285 del 17 dicembre 2013 ("Disposizioni di vigilanza per le banche") e introducendo le specifiche disposizioni riguardanti il whistleblowing.

- I mezzi di segnalazione interna devono **garantire la riservatezza e la protezione dei dati del segnalante/segnalato.**
- Le segnalazioni **devono avere un canale specifico ed autonomo rispetto alle normale linee di reporting.**
- I soggetti preposti alla ricezione, all'esame e alla valutazione delle segnalazioni non siano coinvolti in relazione a eventuali procedimenti decisionali, che saranno attribuiti alle funzioni o agli organi aziendali competenti**. No conflitti d'interesse.**
- Le banche nominano **un responsabile dei sistemi interni di segnalazione per garantire il corretto svolgimento del procedimento.**
- L'adozione di una specifica **procedura in materia**.

SUL PUNTO SI VEDA ANCHE L'ABI

Whistleblowing e D.Lgs 231/2001: alcune normative parallele

DISCIPLINA ANTIRICICLAGGIO

Il whistleblowing è espressamente disciplinato anche nell'ambito della normativa di contrasto al riciclaggio e al finanziamento del terrorismo. Con il recepimento della quarta direttiva europea (Dir. UE 2015/849), ad opera del D.Lgs. 90/2017, il legislatore nazionale ha infatti introdotto nel D.Lgs. 231/2007 il Capo VII ("segnalazione di violazioni") e, al suo interno, l'art. 48 ("segnalazione di violazioni")

- **La tutela della riservatezza dell'identità del segnalante e del presunto responsabile delle violazioni**, ferme restando le regole che disciplinano le indagini e i procedimenti avviati dall'autorità giudiziaria in relazione ai fatti oggetto delle segnalazioni.
- **La tutela del soggetto che effettua la segnalazione contro condotte ritorsive, discriminatorie** o comunque sleali conseguenti la segnalazione
- **Lo sviluppo di uno specifico canale di segnalazione, anonimo e indipendente**, proporzionato alla natura e alle dimensioni del soggetto obbligato
- L'adozione di una specifica **procedura in materia**.

Whistleblowing e D.Lgs 231/2001: alcune normative parallele

DISCIPLINA SSL

Altro ambito di applicazione della disciplina relativa al whistleblowing riguarda la tutela della salute e della sicurezza dei lavoratori e le attività di prevenzione da attuare sui luoghi di lavoro (cfr. art. 20 d.Lgs 81/2008 che stabilisce stabilisce l'obbligo di "*segnalare immediatamente al datore di lavoro, al dirigente o al preposto le deficienze dei mezzi e dei dispositivi […], nonché qualsiasi eventuale condizione di pericolo di cui vengano a conoscenza, adoperandosi direttamente, in caso di urgenza, nell'ambito delle proprie competenze e possibilità e fatto salvo l'obbligo di cui alla lettera f) per eliminare o ridurre le situazioni di pericolo grave e incombente, dandone notizia al rappresentante dei lavoratori per la sicurezza*").

DISCIPLINA CONCORRENZA E ANTITRUST

Per ciò che concerne l'ambito della tutela della concorrenza, in assenza di una specifica disposizione normativa, uno dei principali elementi cui far riferimento può essere rinvenuto nella Comunicazione della Commissione Europea del 16 marzo 2017, nell'ambito della quale si esprime la volontà di dare vita a un nuovo strumento che renda più facile inviare segnalazioni relative a eventuali cartelli e altre violazioni della normativa antitrust, mantenendo comunque l'anonimato.

DISCIPLINA ASSICURATIVA

Per ciò che concerne il settore assicurativo, l'istituto in questione è stato disciplinato ad opera del D.Lgs. 68/2018, che ha introdotto gli artt. 10-quater e 10-quinquies nel D.Lgs. 209/2005

ODCEC m@ster®

ORDINE DEI DOTTORI COMMERCIALISTI E DEGLI ESPERTI CONTABILI
MILANO

FONDAZIONE COMMERCIALISTI ODCEC di MILANO

Whistleblowing: rapporti con la normativa sulla privacy (GDPR)

Whistleblowing: rapporti con la normativa sulla privacy (GDPR)

- Necessità di fornire una corretta **informativa** privacy
- Valutare i corretti **tempi di conservazione** soprattutto nel caso di utilizzo di applicativi software (attenzione alle wp 117 che forniscono delle indicazioni a riguardo e che deve essere letto con l'art. 13 e 5 in materia di limitazione della conservazione del GDPR)
- Garantire **l'esercizio dei diritti** previsti ex art. 15 e ss. del GDPR (attenzione alla limitazione dell'esercizio dei diritti previsto all'art. 2 *undecies* del D.Lgs 101/2018)
- Adottare un **sistema organizzativo interno** (lettere di autorizzazione) che garantisca la segregazione delle funzioni e dei compiti nonché la conoscenza dei dati del segnalante/segnalato solo a determinate figure identificate
- Gestire correttamente il **rapporto con eventuali outsourcer informatici** (nomina ex art. 28, verifica delle misure tecniche adottate per garantire la riservatezza del segnalante etc.) sia nel caso in cui la procedura informatica di acquisizione e gestione delle segnalazioni risieda presso il titolare sia nel caso in cui venga fornita in modalità "software as a service"
- Adozione di misure tecniche con particolare riguardo all'art. 32 del GDPR e verifica dell'eventuale necessità di svolgimento di **DPIA**

Whistleblowing e privacy: alcune sanzioni del Garante Privacy

Ordinanza ingiunzione nei confronti di Aeroporto Guglielmo Marconi di Bologna

Principali contestazioni:

- Mancato utilizzo di **tecniche crittografiche** per il trasporto e la conservazione dei dati;
- **Tracciamento degli accessi** (anche dei segnalanti) all'applicativo;
- Mancata esecuzione di una **valutazione d'impatto** sulla protezione dei dati;
- Mancata adozione di un **protocollo di rete sicuro** (quale il protocollo https);
- Mancata regolarizzazione **ruolo del sub responsabile**.

40.000 €

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9685922

Provvedimento correttivo e sanzionatorio nei confronti di Università degli studi di Roma "La Sapienza"

Principali contestazioni:

- **Sicurezza** del trattamento;
- Le misure tecniche per il **controllo degli accessi**;
- **Misure tecniche** per il trasporto e la conservazione dei dati.

40.000 €

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9269618

Whistleblowing e privacy: alcune sanzioni del Garante Privacy

Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022 [9768363]

Adempimenti in materia di protezione e tutela dei dati personali connessi all'**utilizzo di software per il c. d. whistleblowing**.

Principali punti di attenzione :

1. Fornire **preventivamente adeguata informativa** ai soggetti segnalanti sui dati trattati per la finalità di segnalazione degli illeciti;
2. Provvedere all'aggiornamento del **registro dei trattamenti**;
3. Condurre una valutazione di impatto (**DPIA**);
4. Regolare i rapporti privacy con il fornitore, il quale nel caso di specie si configura Responsabile del trattamento, provvedendo alla **nomina ex art. 28 GDPR**.

Ulteriori elementi di attenzione sollevati dal Garante:

1. L'accesso all'applicazione web di whistleblowing, basata su software open source, avveniva attraverso sistemi che, non essendo stati correttamente configurati, **registravano e conservano i dati di navigazione degli utenti (c. d. "log"), consentendo l'identificazione degli interessati**, tra cui i potenziali segnalanti, risultando così carente l'adozione di misure tecniche ed organizzative e rendendo inefficaci le altre misure implementate al fine di tutelare la riservatezza dell'identità dei soggetti segnalanti;
2. Le modalità di **gestione delle credenziali di autenticazione** per l'accesso all'applicativo in questione non risultavano adeguate sotto il profilo della sicurezza.

40.000 €

Whistleblowing e privacy: la conservazione dei dati

Linee guida CNIL del 18.07.2019

Nella fase di acquisizione della segnalazione il titolare deve fare in modo che il segnalante inserisca solo i dati necessari

Parere 1/2006 relativo all´applicazione della normativa UE sulla protezione dei dati alle procedure interne per la denuncia delle irregolarità riguardanti la tenuta della contabilità, i controlli contabili interni, la revisione contabile, la lotta contro la corruzione, la criminalità bancaria e finanziaria 1 febbraio 2006 - WP 117

Nella fase di istruzione ed indagine il titolare deve conservare e trattare solo le informazioni necessarie

Parere sullo schema di "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 (c.d. whistleblowing)" - 4 dicembre 2019 [9215763]

Il titolare del trattamento è chiamato a fissare la durata del periodo di conservazione per il trattamento dei dati personali raccolti durante la procedura di segnalazione

La disciplina del whistleblowing: indicazioni e spunti operativi per i professionisti del 12 febbraio 2021

Il periodo di conservazione può variare in funzione dell'esito del processo di segnalazione

Diritto degli interessati di conoscere modalità e la misura con cui sono o saranno trattati i dati personali che li riguardano

Whistleblowing e privacy: ruoli e rapporti

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231

VEDI ANCHE Newsletter del 21 maggio 2020

AODV 231
Associazione dei Componenti degli Organismi di Vigilanza ex d.lgs. 231/2001

Parere sulla qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza previsti dall'art. 6, d.lgs. 8 giugno 2001, n. 231

1. Quesito

Con nota del 16 ottobre 2019, l'Associazione dei Componenti degli Organismi di Vigilanza ex d.lgs. 231/2001 (di seguito, Associazione), ha chiesto all'Autorità un incontro per discutere della qualificazione soggettiva ai fini privacy degli Organismi di Vigilanza (di seguito, OdV). Nel corso dell'incontro, che si è svolto presso la sede del Garante in data 5 novembre 2019, l'Associazione ha rappresentato la propria posizione in merito, illustrando quanto contenuto in un position paper approvato dal Consiglio Direttivo il 21 marzo 2019. In tale documento l'Associazione, dopo aver analizzato le diverse tesi emerse in dottrina, ha concluso sostenendo che "l'OdV in quanto parte dell'impresa", non sia qualificabile né come titolare né come responsabile del trattamento, [...e che] ai fini dell'osservanza delle norme relative alla protezione dei dati l'inquadramento soggettivo dell'Organismo di Vigilanza [...] sia assorbito da quello dell'Ente/società vigilata della quale, appunto, l'OdV è "parte".

Successivamente all'incontro, l'Associazione ha trasmesso in data 11 novembre e 20 dicembre 2019 ulteriore documentazione sull'argomento e una memoria di approfondimento a supporto della tesi sostenuta.

2. La disciplina in materia di protezione dei dati personali: Regolamento (UE) 2016/679, decreto legislativo n. 196/2003 come novellato dal d.lgs. 10 agosto 2018 n. 101

Il Regolamento (UE) 2016/679 (di seguito, Regolamento) si pone in linea di continuità con quanto previsto dalla Direttiva 95/46/CE (di seguito, Direttiva) rispetto all'individuazione dei ruoli di titolare e responsabile e alla distribuzione delle relative responsabilità.

Infatti, con definizione sostanzialmente sovrapponibile a quella contenuta nella Direttiva (art. 2, lett. d)), il Regolamento definisce "titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali" (art. 4, n. 7) e "responsabile del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento" (art. 4, n. 8).

Alla luce delle definizioni sopra riportate, pertanto, il titolare è il soggetto sul quale ricadono le decisioni di fondo relativamente alle finalità e alle modalità del trattamento dei dati personali degli interessati e che, nell'ambito della predisposizione delle misure tecniche e organizzative volte a soddisfare i requisiti stabiliti dal Regolamento (c.d. principio di accountability), anche sotto il profilo della sicurezza, può ricorrere ad uno o più responsabili, individuati tra soggetti particolarmente qualificati per lo svolgimento di alcune attività di trattamento (cons.81 del Regolamento). Il responsabile svolge attività per conto del titolare, agendo sulla base di finalità eterodeterminate dal titolare e nell'interesse di questo (v. Gruppo art. 29 Wp 169 del 16 febbraio 2010 sui concetti di "responsabile e incaricato del trattamento") e, nell'ambito delle attività allo stesso delegate, è tenuto ad agire attenendosi alle istruzioni impartite dal titolare del trattamento.

*'Sulla base delle valutazioni sopra riportate, si ritiene che **l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongano siano interni o esterni**, debba essere considerato **"parte dell'ente".** Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti dalla legge, attraverso il riconoscimento di "autonomi poteri di iniziativa e controllo" - si svolge nell'ambito dell'organizzazione dell'ente, titolare del trattamento, che, attraverso la predisposizione dei modelli di organizzazione e di gestione, definisce il perimetro e le modalità di esercizio di tali compiti. Tale posizione si intende ricoperta dall'OdV nella sua collegialità, tuttavia, non può prescindersi dalla necessità di definire anche il ruolo che, in base alla disciplina in materia di protezione dei dati personali, deve essere previsto per i singoli membri che lo compongono. **Lo stesso ente, in ragione del trattamento dei dati personali che l'esercizio dei compiti e delle funzioni affidate all'OdV comporta** (ad esempio, l'accesso alle informazioni acquisite attraverso flussi informativi), **designerà** - nell'ambito delle misure tecniche e organizzative da porre in essere in linea con il principio di accountability (art. 24 del Regolamento) - **i singoli membri dell'OdV quali soggetti autorizzati** (artt. 4, n. 10, 29, 32 par. 4 Regolamento; v. anche art. 2-quaterdecies del Codice).'*

https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/9347842

Whistleblowing e privacy: ruoli e rapporti

*'Inoltre, si osserva che, **in base al principio della "protezione dei dati fin dalla progettazione"** (art. 25, par. 1, del Regolamento), il titolare del trattamento deve adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati (art. 5 del Regolamento) e **deve integrare nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati**. **Tale obbligo si estende anche ai trattamenti svolti per mezzo di un responsabile del trattamento**. Infatti, le **operazioni di trattamento effettuate da un responsabile dovrebbero essere regolarmente esaminate e valutate dal titolare per garantire che continuino a rispettare i principi e permettano al titolare di adempiere gli obblighi previsti dal Regolamento**. **(Ordinanza ingiunzione nei confronti di Azienda ospedaliera di Perugia - 7 aprile 2022 [9768363]***

Nello svolgimento dell'attività può comunicare i dati al Responsabile al fine di trattarli per Suo conto. (si veda definizione art. 4 (8) GDPR)

I — **Poiché il Titolare del trattamento nomina Responsabili al trattamento solo quei soggetti che presentano garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate, risulterà fondamentale, anche ai fini delle esimenti in materia di culpa in eligendo, prevedere una check list che valuti ed attesti le misure organizzative e di sicurezza dei soggetti nominati.**

II — **Sulla scorta del art. 28 del GDPR, al fine di rispettare il principio di accountability, risulterà fondamentale prevedere un apposito contratto o altro atto giuridico all'interno del quale il Titolare del Trattamento specifici quanto contenuto al comma 3 art. 28 GDPR.**

III — **Risulterà fondamentale, se vi è una base contrattuale alla quale l'atto di nomina si allega, prevedere una clausola contrattuale che vada a sostituire quella già esistente integrata ed innovata con il GDPR e il D.Lgs 101/2018 che dia evidenza del ruolo tra le parti.**

IV — **Risulterà infine fondamentale, procedere a valutazione periodica del Soggetto nominato come Responsabile al fine di verificare l'adeguatezza e la veridicità delle misure attestate in fase di nomina e la tenuta del processo di designazione.**

Whistleblowing e privacy: gli adempimenti privacy

Privacy by design

Valutazione di Impatto (DPIA)

Il sistema di gestione delle segnalazioni deve essere sottoposto a DPIA preliminare.

Accountability

Aggiornamento registro trattamenti e ruoli interni

Il trattamento va censito nel registro e l'organismo preposto va autorizzato

Regolarizzazione ruolo Fornitori

I fornitori di piattaforme, software e servizi (es. ethic point) devono essere designati responsabili del trattamento. Anche il ruolo dei sub fornitori va regolarizzato.

Trasparenza

Presidi informativi

Occorre predisporre un'informativa sul trattamento ed una procedura di gestione delle segnalazioni.

Sicurezza dei trattamenti

Misure di sicurezza

L'Azienda è responsabile dell'individuazione delle misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti

CONTATTI

Dott. Federico Temporiti
Senior Manager / Advisory Risk & Compliance
+39 345 2954748
federico.temporiti@bdo.it

Avv. Martina Pesenti
Supervisor / Advisory Risk & Compliance
+39 340 5986251
martina.pesenti@bdo.it

BDO Advisory Services S. r. l.
Viale Abruzzi, 94
20131 Milano