

La responsabilità amministrativa degli enti ex D. Lgs. 231/2001

LA DISCIPLINA DEL WHISTLEBLOWING

Dott. Federico Temporiti
Avv. Martina Pesenti
Avv. Marco Lorusso

13 ottobre 2023



GLI IMPATTI DEL D.LGS. 24/2023 SULL'AGGIORNAMENTO DEL MODELLO 231



LA TUTELA DEL SEGNALANTE TRA RISERVATEZZA E RISPETTO DELLA DISCIPLINA SULLA *PRIVACY*



GLI IMPATTI DEL D.LGS. 24/2023 SULL'AGGIORNAMENTO DEL MODELLO 231



LA TUTELA DEL SEGNALANTE TRA RISERVATEZZA E
RISPETTO DELLA DISCIPLINA SULLA *PRIVACY*

Entrata in vigore

Con l'entrata in vigore del D. Lgs. 24/2023 a far data dal [15 luglio 2023](#), le disposizioni normative hanno trovato applicazione:

a tutte le Società con più di 250 dipendenti.

Con l'entrata in vigore del D. Lgs. 24/2023 a far data dal [17 dicembre 2023](#) troveranno applicazione le disposizioni normative in materia di whistleblowing:

a tutte le Società con più di 50 dipendenti;

a tutte le Società che abbiano già adottato un modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/2001, a prescindere dalla loro dimensione.

Breve panoramica sul recente d. Lgs. 24/2023

<p>Efficacia del D.lgs. n. 24/2023</p> <p>Tutti gli enti del settore pubblico e gli enti del settore privato con più di 250 dipendenti impiegati nell'ultimo anno devono adeguarsi entro il 15 luglio 2023.</p> <p>Gli enti del settore privato con dipendenti compresi tra 50 e 249 impiegati nell'ultimo anno e quelli con meno di 50 dipendenti che hanno già un Modello 231 o che operano nell'ambito degli atti dell'Unione di cui agli allegati I.B e II (cfr. nota 1) del D.lgs. 24/2023 devono adeguarsi a partire dal 17 dicembre 2023.</p>	<p>Ambito di applicazione oggettivo</p> <p>Ampliamento dell'ambito di applicazione oggettivo, che ricomprende tutti gli atti, gli illeciti e le violazioni che ledono l'interesse pubblico e l'integrità dell'ente.</p> <p>Restano esclusi quelli che impattano su fattori diversi, come le contestazioni, le richieste e le rivendicazioni personali.</p>	<p>Ambito di applicazione soggettivo</p> <p>Ampliamento dell'ambito di applicazione soggettiva, che ricomprende lavoratori subordinati e autonomi, collaboratori, consulenti, liberi professionisti, volontari, tirocinanti e così via, nonché i cc.dd. «facilitatori», chi lavora nello stesso contesto del segnalante, i parenti entro il quarto grado e così via.</p>
<p>Il canale di segnalazione interna</p> <p>Ciascun ente pubblico o privato è tenuto ad istituire un canale di segnalazione interna, che permetta segnalazioni sia scritte che orali.</p>	<p>Il canale di segnalazione esterna</p> <p>Si tratta del canale di segnalazione gestito direttamente dall'ANAC, al quale il segnalante può rivolgersi in presenza di specifiche circostanze (ad es., mancata presa in carico della segnalazione interna).</p>	<p>La divulgazione pubblica</p> <p>Assoluta novità introdotta dal decreto in esame, a cui il segnalante può ricorrere in presenza di circostanze tipiche.</p>

Breve panoramica sul recente d. Lgs. 24/2023

<p>Il ruolo dell'ANAC</p> <p>Anzitutto, l'ANAC gestisce il canale di segnalazione esterna.</p> <p>Inoltre, rientra tra i soggetti a cui i segnalanti possono denunciare il fatto di aver subito ritorsioni.</p> <p>Infine, dispone del potere di irrogare sanzioni.</p>	<p>L'obbligo di riservatezza</p> <p>Rappresenta uno dei principi cardine del nuovo decreto legislativo e prevede, anche attraverso il ricorso a soluzioni crittografiche, la riservatezza dell'identità del segnalante, della persona coinvolta, dei soggetti a vario titolo menzionati e dell'intera documentazione.</p>	<p>Il trattamento dei dati personali</p> <p>Gli impatti che il nuovo decreto ha sulla protezione dei dati personali sono molteplici e coincidono con la nomina degli autorizzati, la nomina di eventuali responsabili esterni del trattamento, l'obbligo dell'informativa, il rispetto del principio di minimizzazione, l'aggiornamento del registro dei trattamenti, la definizione di un periodo di retention adeguato e, soprattutto, l'obbligo della DPIA.</p>
<p>Le segnalazioni anonime</p> <p>Deve essere concessa al segnalante la possibilità di inviare una segnalazione in forma anonima, fermo restando che, in caso di successiva rivelazione della sua identità, allo stesso si applichino le tutele previste dal decreto in esame.</p>	<p>Le tutele per il segnalante</p> <p>Al fine di incentivare le segnalazioni, il decreto in esame ha previsto il divieto di ritorsione nei confronti del segnalante, l'inversione dell'onere della prova e l'obbligo di riservatezza della sua identità.</p>	<p>Le sanzioni</p> <p>Il potere di irrogare sanzioni è stato affidato all'ANAC e queste possono arrivare sino a 50.000€.</p> <p>È prevista una sanzione anche nei confronti dei segnalanti.</p>

Il D. Lgs. 24/2023 – Cosa cambia?

Le modifiche apportate dal D.Lgs. 24/2023 riguardano i seguenti aspetti:

- I. ampliamento dei soggetti segnalanti;
- II. ampliamento delle condotte segnalabili, che comprenderanno quelle rilevanti in ambito D.Lgs. 231;
- III. ampliamento delle garanzie di protezione per il segnalante e del divieto di ritorsione;
- IV. sistema disciplinare che dovrà ricomprendere non solo le violazioni del MOG ma anche le altre violazioni oggetto del Decreto attuativo.



231 MODELLO ORGANIZZATIVO AI SENSI DEL D.LGS 231/2001

Quali violazioni possono essere segnalate

PRINCIPIO GENERALE :

possono essere segnalate violazioni di disposizioni normative che **ledono l'interesse pubblico** o **l'integrità** dell'ente pubblico o privato commesse nell'ambito del **contesto lavorativo pubblico** o **privato** con cui il segnalante intrattiene un dato rapporto giuridico.

VIOLAZIONI DEL DIRITTO NAZIONALE

illeciti penali, civili, amministrativi o contabili

condotte illecite previste dal D.lgs. n. 231/2001

prescrizioni contenute nel Modello 231 dell'ente

Ad esempio:

- 1) assunzioni non trasparenti;
- 2) false dichiarazioni;
- 3) irregolarità contabili;
- 4) evasione fiscale;
- 5) omesso versamento delle ritenute previdenziali;
- 6) omissione colposa di cautele contro infortuni sul lavoro.

Ad esempio:

- 1) illegale ripartizione degli utili e delle riserve;
- 2) riciclaggio;
- 3) autoriciclaggio;
- 4) emissione di fatture o altri documenti per operazioni inesistenti;
- 5) occultamento o distruzioni di documenti contabili.

Ad esempio:

- 1) violazione del Codice Etico;
- 2) violazione di principi e procedure previste dal Modello 231;
- 3) omessa redazione di documentazione richiesta dal Modello 231;
- 4) ostacolo all'attività di controllo dell'OdV.

Quali violazioni possono essere segnalate

PRINCIPIO GENERALE :

possono essere segnalate violazioni di disposizioni normative che **ledono l'interesse pubblico** o **l'integrità** dell'ente pubblico o privato commesse nell'ambito del **contesto lavorativo pubblico** o **privato** con cui il segnalante intrattiene un dato rapporto giuridico.

atti/omissioni che ledono il mercato interno e la libera circolazione di merci, persone, servizi e capitali

VIOLAZIONI DEL DIRITTO COMUNITARIO

atti/comportamenti che vanificano oggetto o finalità di disposizioni UE nei settori di cui si è detto

Violazioni diritto UE in materia di concorrenza e di aiuti di Stato, di imposta sulle società e i meccanismi il cui fine è ottenere un vantaggio fiscale che vanifichi l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società.

violazione del diritto dell'UE in specifici settori

atti/omissioni che ledono gli interessi finanziari dell'UE

Ad esempio, il caso di un'impresa in posizione dominante, che ricorre a pratiche commerciali abusive (come adozione di prezzi cd. *predatori*, sconti target, vendite abbinate) al fine di pregiudicare la libera e leale concorrenza.

Ad esempio:

- 1) riciclaggio di denaro;
- 2) corruzione negli appalti pubblici dell'UE;
- 3) reati ambientali;
- 4) adozione di pratiche commerciali sleali.

Ad esempio:

- 1) frode;
- 2) corruzione;
- 3) qualsiasi altra attività illegale connessa alle spese UE.

Quali violazioni possono essere segnalate

PRINCIPIO GENERALE :

possono essere segnalate violazioni di disposizioni normative che **ledono l'interesse pubblico** o **l'integrità** dell'ente pubblico o privato commesse nell'ambito del contesto lavorativo pubblico o **privato** con cui il segnalante intrattiene un dato rapporto giuridico.

VIOLAZIONI NON SEGNALABILI

contestazioni,
rivendicazioni e richieste
meramente personali del
segnalante

Ad es., vertenze di lavoro, discriminazioni tra colleghi, conflitti interpersonali tra il segnalante e un altro lavoratore o con i superiori gerarchici e così via

violazioni per cui il diritto
nazionale o dell'Unione già
prevedono procedure di
segnalazione

Ad es., le procedure di segnalazione degli abusi di mercato previste dal Reg. UE n. 596/2014 oppure gli artt. 52-bis e 52-ter del TUB che contengono disposizioni sulle segnalazioni di violazioni nel settore bancario e così via

violazioni in materia di
sicurezza nazionale ed
appalti relativi alla difesa
o sicurezza nazionale

Appalti previsti agli artt. 15 e 24 delle direttive 24 e 25 del 2014, nonché all'art. 13 della direttiva del 2009/81 e che sono esclusi anche dall'ambito di applicazione del codice appalti di cui al d.lgs. n. 36/2023 che rinvia anche al d.lgs. n. 208/2011

Chi può effettuare una segnalazione

Lavoratori subordinati	Si pensi, ad es., a rapporti di lavoro a tempo parziale, intermittente, a tempo indeterminato e determinato, di somministrazione, di apprendistato, di lavoro accessorio, nonché a lavoratori occasionali
Lavoratori autonomi	Si pensi, ad es., a rapporti di agenzia, di rappresentanza commerciale ed altri rapporti di collaborazione (avvocati, ingegneri, assistenti sociali)
Liberi professionisti e consulenti	Si tratta di tutti quei soggetti che prestano la propria attività e che potrebbero trovarsi in posizione privilegiata per segnalare le violazioni di cui sono testimoni
Volontari e tirocinanti	Le segnalazioni possono essere effettuate sia nel caso in cui siano soggetti retribuiti che non retribuiti
Azionisti	Si tratta di soggetti che detengono azioni in società private e che vengono a conoscenza di violazioni nell'esercizio dei diritti di cui sono titolari
Ruoli di amministrazione, direzione, controllo, vigilanza, rappresentanza	Si tratta, ad es., dei componenti dei Consigli di Amministrazione oppure dei componenti degli Organismi di Vigilanza

Le tutele per il segnalante

DIVIETO DI RITORSIONE

L'ente pubblico o la società privata che ricevono una segnalazione sono interessati dal **divieto assoluto di assumere atteggiamenti** o adottare **provvedimenti ritorsivi** nei confronti del segnalante. A mero titolo esemplificativo, sono vietati:

- il licenziamento;
- la sospensione;
- la mancata promozione;
- la riduzione dello stipendio;
- la modifica dell'orario di lavoro;
- le referenze negative;
- l'adozione di misure disciplinari o di sanzioni pecuniarie;
- l'intimidazione;
- l'ostracismo;
- la discriminazione;
- il trattamento sfavorevole.

OBBLIGO DI RISERVATEZZA

La riservatezza, oltre che rispetto all'**identità** del segnalante, viene garantita rispetto a **qualsiasi altra informazione o elemento** della segnalazione idonei da identificare il segnalante.

L'ente garantisce la riservatezza attraverso, ad esempio, l'impiego di una piattaforma informatica crittografata e con accessi consentiti ai soli soggetti autorizzati.

INVERSIONE ONERE DELLA PROVA

La **connessione** tra la ritorsione e la segnalazione **SI PRESUME PER LEGGE**, con la conseguenza che spetterà al datore di lavoro dimostrare che la misura ritorsiva sarebbe stata adottata a prescindere dalla segnalazione.

L'impianto sanzionatorio

Da 10.000 a 50.000 €

- In caso di accertamento di **ritorsioni** poste in essere nei confronti del segnalante;
- In caso di accertamento del fatto che il colpevole abbia ostacolato o tentato di **ostacolare la segnalazione**;
- In caso di accertamento di violazione da parte del colpevole dell'**obbligo di riservatezza**;
- In caso di accertamento di mancata istituzione del **canale di segnalazione**;
- In caso di accertamento di **assenza di procedure** per l'effettuazione o la gestione delle segnalazioni oppure adozione di **procedure non conformi**.

Da 500 a 2.500 €

- Quando è accertata con sentenza di primo grado la responsabilità civile del **segnalante** per **diffamazione** o **calunnia** nei casi di dolo o colpa grave, eccetto il caso in cui sia già intervenuta una condanna di primo grado per i medesimi reati.

Il compito di
applicare le sanzioni
elencate spetta ad
ANAC

Whistleblowing e D.Lgs. 231/2001

La gestione del whistleblowing all'interno delle imprese private è da sempre legata al D. Lgs. 231/2001.

La [Legge 179/2017](#), regolamentando la tutela degli autori di segnalazioni di reati o irregolarità in ambito pubblico o privata, aveva imposto alle organizzazioni che avevano scelto di adottare Modelli Organizzativi 231, l'obbligo di implementare canali di segnalazioni tali da proteggere contro atti ritorsivi.



Questo binomio tra normativa 231/2001 e whistleblowing è stato in parte superato dal [D. Lgs. 24/2023](#), entrato in vigore il 30 marzo 2023.

La principale novità introdotta riguarda la circostanza che l'applicazione dell'istituto non viene più limitata alle violazioni rilevanti ai sensi del Decreto 231 ma si estende fino a ricomprendere violazioni del diritto nazionale e dell'UE.

Come cambia il Modello 231?

Il D. Lgs. 24/2023 ha riformato in maniera strutturale la materia del whistleblowing incidendo sul Modello organizzativo e di conseguenza sul ruolo dell'Odv.

Nello specifico:

- L'articolo 4 co. 1 del Decreto 24 prevede espressamente che « (...) i *modelli di organizzazione e di gestione, di cui all'art. 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto*».
- L'art. 24 del Decreto 24 modifica l'art. 6 co. 2-bis del D.Lgs. 231/2001 disponendo che i modelli prevedano:
 - canali di segnalazione interna atti a garantire, con modalità informatiche, la riservatezza del segnalante
 - il divieto di atti di ritorsione o discriminatori nei confronti del segnalanti per motivi collegati alla segnalazione
 - il sistema disciplinare che preveda sanzioni nei confronti di chi viola le misure di tutela del segnalante, nonché di chi effettua con dolo o colpa grave delle segnalazioni che si rivelino infondate
- L'art. 21 del Decreto 24 invece dispone che le Società che hanno adottato il Modello 231 prevedano, nel sistema disciplinare, delle **sanzioni** per coloro che sono stati ritenuti responsabili di alcuni comportamenti, ovvero abbiano commesso ritorsioni o ostacolato le segnalazioni; non abbiano adottato procedure per l'effettuazione e gestione delle segnalazioni; abbia commesso reati di diffamazione.

Aggiornamento del Modello 231

L'aggiornamento dovrà riguardare complessivamente il Modello (nella parte generale ma anche nel Codice Etico) andando ad armonizzare quanto imposto dalla novella legislativa con il sistema preesistente.

Allo stesso modo le Società dovranno adottare *policy ad hoc* per gestire le segnalazioni, avendo cura di disciplinare i seguenti aspetti:

- le normative di riferimento
- le violazioni segnalabili
- i ruoli e le responsabilità dei soggetti incaricati di gestione le segnalazioni
- il canale di segnalazione interna
- il canale di segnalazione esterna e la divulgazione pubblica
- il processo di gestione delle segnalazioni
- gli adempimenti privacy necessari
- le tutele per il segnalante
- la conservazione della documentazione
- l'impianto sanzionatorio

Ruolo dell'Organismo di Vigilanza

Dall'inserimento dei canali di segnalazione interna nel Modello, dipendono dei compiti per l'Organismo di Vigilanza che è tenuto a:

- vigilare sulla tempestiva adozione dei canali di segnalazione interna e sul conseguente aggiornamento del mog
- vigilanza sull'avvenuta adozione delle procedure di gestione delle segnalazioni
- vigilare sulla formazione e informazioni e diffusione delle procedure e del mog aggiornato
- vigilare sull'accessibilità di tali canali di segnalazione



A prescindere dal ruolo di gestore delle segnalazioni che l'Odv può assumere, quest'ultimo deve ricevere alcuni **flussi informativi periodici**:

- dal gestore delle segnalazioni in merito a tutte le segnalazioni al fine di verificare il funzionamento del sistema implementato

Inoltre, deve essere destinatario di **flussi informativi ad evento**:

- laddove ci sia una segnalazione avente rilevanza 231 al fine di compiere le proprie valutazioni in sede di vigilanza e formulare eventuali osservazioni in caso di rilievo di anomalie.

Whistleblowing: alcune domande rilevanti



Cosa si intende per canale di segnalazione?

Quanti canali bisogna predisporre?

Il canale deve essere anonimo o no?

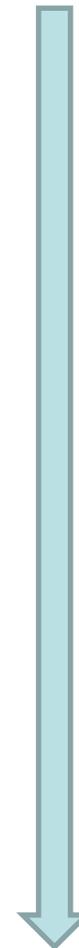
Come tutelare la riservatezza?

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?



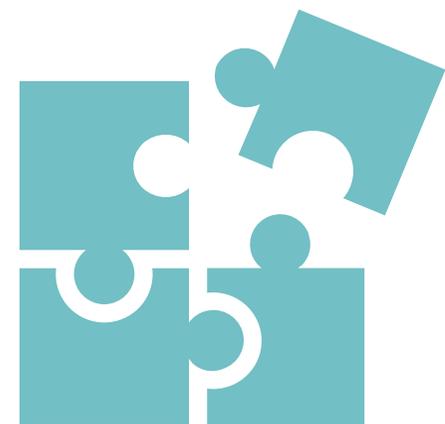


*GLI IMPATTI DEL D.LGS. 24/2023
SULL'AGGIORNAMENTO DEL MODELLO 231*



**LA TUTELA DEL SEGNALANTE TRA RISERVATEZZA E
RISPETTO DELLA DISCIPLINA SULLA PRIVACY**

Whistleblowing: rapporti con la normativa sulla privacy (GDPR)



Framework normativo

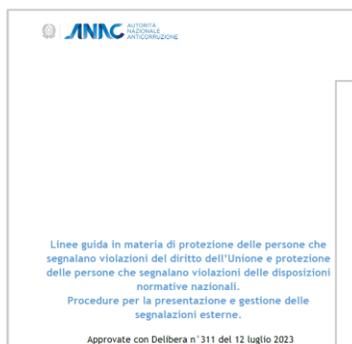
Normativa specifica

- **DECRETO LEGISLATIVO 10 marzo 2023, n. 24**

Normativa tutela dati personali

- **Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 (GDPR)**
- **DECRETO LEGISLATIVO 30 giugno 2003, n.196 ss. mm. ii ('Codice Privacy')**

Supporto interpretativo



Whistleblowing: gli adempimenti privacy

Principi generali

Informativa e consenso

Soggetti del trattamento

Ulteriori adempimenti

Sicurezza

II DECRETO LEGISLATIVO 10 marzo 2023, n. 24, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali dedica specifiche previsioni normative agli aspetti di tutela e protezione dei dati personali.

Whistleblowing: gli adempimenti privacy



Garantire il principio di **minimizzazione**

Definire il periodo e le modalità di **conservazione** dei dati

Le segnalazioni e la relativa documentazione sono conservate non oltre 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione.

Garantire il rispetto del principio di **Privacy by Design & Default**

Garantire la **riservatezza dell'identità del segnalante e del segnalato** secondo le logiche descritte dall'art. 12 D. 24/2023

Whistleblowing: gli adempimenti privacy



Predisporre e formalizzare **informativa privacy** da rendere agli interessati (segnalanti e segnalati), definendone le modalità di trasmissione

Richiedere il **consenso** del segnalante per rivelare la sua identità a persone diverse dai soggetti autorizzati a gestire la segnalazione

Rispettare i principi di cui all'art. 14 c. 2-4 in caso di segnalazioni tramite linee telefoniche o segnalazioni effettuate oralmente.

Whistleblowing: gli adempimenti privacy



Definire la **responsabilità della gestione** e del funzionamento del sistema di whistleblowing, in particolare di eventuali **terze parti** (es. fornitori di piattaforme di segnalazione) inquadrabili come **responsabili del trattamento**.



Impartire specifiche e adeguate **istruzioni** ai soggetti autorizzati al trattamento nell'ambito del sistema di segnalazione ed erogare la **formazione** ai soggetti autorizzati al trattamento nell'ambito del sistema di segnalazione

Laddove siano condivise risorse per il ricevimento e la gestione delle segnalazioni tra più soggetti, gli stessi determinano in modo trasparente, mediante un **accordo interno, le rispettive responsabilità** in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 GDPR

Whistleblowing: gli adempimenti privacy



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 180 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.

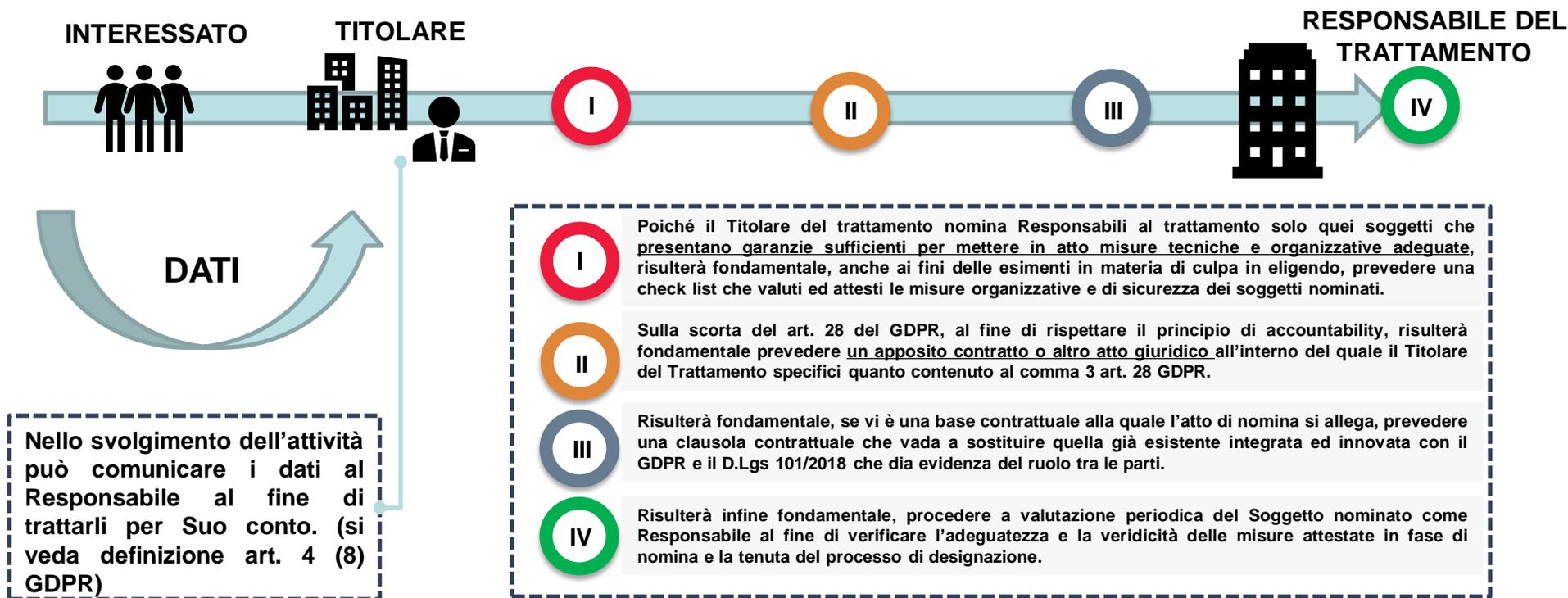
'Sulla base delle valutazioni sopra riportate, si ritiene che l'OdV, nel suo complesso, a prescindere dalla circostanza che i membri che lo compongono siano interni o esterni, debba essere considerato "parte dell'ente". Il suo ruolo - che si esplica nell'esercizio dei compiti che gli sono attribuiti 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 prescindere 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: gli adempimenti privacy

‘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])



Whistleblowing: gli adempimenti privacy



Effettuare un'**analisi dei rischi** e condurre una **DPIA** finalizzata, tra l'altro, ad individuare misure tecniche e organizzative

Aggiornare il **registro dei trattamenti**

Mappare i **trasferimenti** verso paesi terzi e le relative garanzie a supporto

Garantire l'**esercizio dei diritti** agli interessati, nei limiti di quanto previsto dall'articolo 2-undecies del Codice Privacy

Definire le procedure in caso di **Data Breach**

Whistleblowing: gli adempimenti privacy



Definire e applicare procedure per la concessione, la modifica e la revoca dell'accesso al sistema whistleblowing

Predisporre misure di sicurezza adeguate per la piattaforma di segnalazione

- procedure di autenticazione basate su tecniche di "strong authentication" (es. OTP)
- utilizzo di protocolli sicuri di trasporto dei dati (https)
- meccanismi di profilazione che consentano solo la visibilità necessaria

Definire le modalità per la manutenzione del sistema di segnalazione

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 €

CONTATTI

Dott. Federico Temporiti

Senior Manager / Advisory Risk &
Compliance

+39 345 2954748

federico.temporiti@bdo.it

Avv. Martina Pesenti

Manager / Advisory Risk &
Compliance

+39 340 5986251

martina.pesenti@bdo.it

Avv. Marco Lorusso

Specialist / Compliance
Department

+39 347 6226704

marco.lorusso@bdo.it

BDO Advisory Services S. r. l.

Viale Abruzzi, 94

20131 Milano