

MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D.LGS. 231/2001 E S.M.I.

Approvato dal Consiglio di Amministrazione del 11 novembre 2026

POLICY WHISTLEBLOWING

INDICE

1. DEFINIZIONI ... 3
2. PREMESSA ... 5
3. OBIETTIVI DEL DOCUMENTO ... 6
4. AMBITO DI APPLICAZIONE SOGGETTIVO ... 6
5. DIFFUSIONE, INFORMAZIONE E FORMAZIONE ... 7
6. MODALITÀ OPERATIVE ... 7
6.1. I diversi canali di segnalazione ... 7
6.1.1. Canali interni ... 8
6.1.2. La gestione della Segnalazione tramite i canali interni ... 8
6.1.3. GESTIONE SEGNALAZIONI ANONIME ... 13
6.1.4. Canale esterno ... 14
6.1.5. Divulgazione pubblica ... 15
6.2. DENUNCIA ALL'AUTORITÀ GIURISDIZIONALE ... 16
6.3. I CONTENUTI DELLA SEGNALAZIONE ... 16
6.4. LE TUTELE ... 19
6.4.1. L'obbligo di riservatezza ... 19
6.4.2. Il divieto di Ritorsione ... 20
6.4.3. La protezione in caso di Ritorsioni ... 22
6.4.4. Ulteriori misure a favore dei Segnalanti ... 23
6.5. PROTEZIONE DATI PERSONALI ... 23
6.6. SANZIONI DISCIPLINARI E ALTRI PROVVEDIMENTI ... 26
6.7. OWNER DELLA POLICY E ARCHIVIAZIONE ... 27
6.8. entrata in vigore e modifiche ... 27

1. DEFINIZIONI

ANAC: Autorità Nazionale Anticorruzione;

Autorità: Autorità Giudiziaria competente;

Codice Privacy: codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196;

Decreto Whistleblowing: il D.lgs. n. 24 del 10 marzo 2023, emanato in attuazione della 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali;

Decreto 231: Decreto Legislativo 8 giugno 2001, n. 231 che disciplina la responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica;

Divulgazione pubblica: modalità seguita dal Segnalante per rendere di pubblico dominio informazioni sulle violazioni tramite la stampa o mezzi elettronici o comunque tramite mezzi di diffusione in grado di raggiungere un numero elevato di persone;

Facilitatore: persona fisica che assiste il Segnalante nel processo di Segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;

GDPR: Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

Modello 231 o **Modello**: Modello di Organizzazione Gestione e Controllo adottato da ASM Terni S.p.A.;

OdV: Organismo di Vigilanza della Società;

Organo Ricevente: Organismo di Vigilanza che riceve la Segnalazione e la gestisce, mantenendo le interlocuzioni con il Segnalante, dando seguito alle Segnalazioni ricevute mediante i canali interni;

Ritorsione: qualsiasi comportamento, provvedimento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della Segnalazione, della denuncia all'Autorità Giudiziaria o della Divulgazione Pubblica, che provoca o può provocare, al Segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto;

Segnalante: persona fisica che effettua la Segnalazione o la divulgazione pubblica di informazioni sulle violazioni; la persona fisica può rientrare in una delle seguenti categorie: (i) dipendenti della Società; (ii) lavoratori autonomi che svolgono la propria attività lavorativa presso la Società; (iii) liberi professionisti e consulenti che prestano la propria attività presso la Società; (iv) volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Società; (v) azionisti (persone fisiche), (vi) persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza presso la Società anche qualora tali funzioni siano esercitate in via di mero fatto;

Segnalazione: comunicazione scritta o orale di informazioni sulle violazioni acquisite;

Società: ASM Terni S.p.A.;

ASM: ASM Terni S.p.A.

2. PREMESSA

Il D.lgs. n. 24 del 10 marzo 2023, emanato in attuazione della 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (di seguito "**Decreto Whistleblowing**") recepisce in Italia la nuova disciplina europea orientata, da un lato, a garantire la manifestazione della libertà di espressione e di informazione, dall'altro, a prevenire e contrastare fenomeni quali la corruzione, la cattiva amministrazione e la prevenzione di violazioni di legge nel settore pubblico e privato.

Chi segnala fornisce informazioni che possono portare all'indagine, all'accertamento e al perseguimento di casi di violazione delle norme, rafforzando i principi di trasparenza e responsabilità.

La disciplina di cui al Decreto Whistleblowing, garantendo la protezione - sia in termini di tutela della riservatezza sia di tutela in caso di ritorsioni - dei soggetti Segnalanti, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per l'ente e di riflesso, per l'interesse pubblico collettivo.

Alla luce della nuova disciplina, ASM Terni S.p.A. (di seguito "**Società**" o "**ASM**") ha adottato la presente Policy al fine di adeguarsi al Decreto Whistleblowing e ciò anche alla luce di quanto previsto nel Modello di Organizzazione Gestione e Controllo (di seguito "**Modello 231**" o "**Modello**") adottato, modificato alla luce della modifica della disciplina in materia di responsabilità degli enti.

ASM, ha redatto la presente Policy quale società a partecipazione mista pubblico-privata, non a controllo pubblico, che, anche in virtù di concessione, gestisce il servizio di distribuzione elettrica, raccolta e trasporto rifiuti urbani e assimilati.

Il Decreto Whistleblowing, infatti, ha sostituito il comma 2-bis dell'art. 6 del D.lgs. n. 231/2001 con il seguente: "*2-bis. I modelli di cui al comma 1, lettera a), prevedono, ai sensi del decreto legislativo attuativo della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare, adottato ai sensi del comma 2, lettera e)*" ed ha abrogato i commi 2-ter e 2 quater.

In ossequio al Decreto Whistleblowing, ogni trattamento di dati personali previsto dalla presente Policy sarà effettuato a norma del GDPR e del Codice Privacy.

3. OBIETTIVI DEL DOCUMENTO

La presente Policy regola il processo di trasmissione, ricezione, analisi e gestione di Segnalazioni di violazioni intese quali comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità della Società, come meglio specificato al successivo Par. 6.3., effettuate dai Segnalanti tramite i diversi canali di segnalazione.

La presente Policy viene adottata alla luce di quanto previsto dal Decreto Whistleblowing, nonché dal Decreto 231.

4. AMBITO DI APPLICAZIONE SOGGETTIVO

La Policy si applica ai cosiddetti Segnalanti che possono essere:

i. dipendenti della Società;

ii. lavoratori autonomi che svolgono la propria attività lavorativa presso la Società;

iii. lavoratori o collaboratori che svolgono la propria attività lavorativa presso la Società;

iv. liberi professionisti e consulenti che prestano la propria attività presso la Società;

v. volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso la Società;

vi. azionisti (persone fisiche),

vii. persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza presso la Società anche qualora tali funzioni siano esercitate in via di mero fatto.

Per tutti i suddetti Segnalanti la tutela si applica anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro o altro rapporto giuridico.

A ciò si aggiunga che le tutele previste per i Segnalanti (cfr. Par. 6.4.) sono estese anche a:

i. facilitatori;

ii. persone del medesimo contesto lavorativo del Segnalante e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado;

iii. colleghi di lavoro del segnalante, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente;

iv. enti di proprietà - in via esclusiva o in compartecipazione maggioritaria di terzi - del Segnalante;

v. enti presso i quali il Segnalante lavora;

vi. enti che operano nel medesimo contesto lavorativo del Segnalante.

5. DIFFUSIONE, INFORMAZIONE E FORMAZIONE

La presente Policy e i diversi canali di segnalazione sono visionabili e messi a disposizione sia tramite pubblicazione della presente nella intranet della Società[1], sia sul sito web[2] alla sezione dedicata al seguente link: Whistleblowing (asmterni.it). - https://www.asmterni.it/trasparenza-prevenzione-della-corruzione-segnalazione-whistleblowing/

Inoltre, la presente viene inviata ad ogni membro del Consiglio di Amministrazione, del Collegio Sindacale e dell'Organismo di Vigilanza della Società da parte del responsabile Unità Legale di ASM.

I contenuti della presente Policy nonché di quanto previsto dal Decreto Whistleblowing saranno oggetto di sessioni formative dedicate rivolte sia a coloro che possono rivestire il ruolo di Segnalanti sia, ove fosse necessario, a coloro che rivestono il ruolo di Organo Ricevente.

L'Unità Risorse Umane assicura la consegna della presente Policy ai dipendenti in servizio in sede di prima applicazione e all'atto dell'assunzione per i nuovi dipendenti, avendo cura di documentarne la presa visione.

6. MODALITÀ OPERATIVE

6.1. I DIVERSI CANALI DI SEGNALAZIONE

La Società, mediante la presente Policy, rende edotti i Segnalanti dei possibili canali mediante i quali, alle condizioni previste dal Decreto Whistleblowing, è possibile eseguire una Segnalazione:

i. canali interni (cfr. Par. 6.1.1.) da considerarsi preferenziali;

ii. un canale esterno da considerarsi residuale ai canali interni nonché da utilizzare nei casi previsti dal legislatore (cfr. Par. 6.1.4.);

iii. divulgazione pubblica da considerarsi residuale ai primi due nonché da utilizzare nei casi previsti dal legislatore (cfr. Par. 6.1.5.).

In via prioritaria, quindi, i Segnalanti sono incoraggiati a utilizzare i canali interni della Società e, solo al ricorrere di certe condizioni, di seguito illustrate, possono essere effettuate le Segnalazioni mediante il canale esterno o mediante la Divulgazione Pubblica.

[1] In tal modo le informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro.
[2] Rendendo così accessibili le informazioni anche alle persone che pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico con la Società.

Inoltre, come previsto dal Decreto Whistleblowing, il Segnalante potrà presentare anche denuncia direttamente all'Autorità competente (cfr. Par. 6.2.).

6.1.1. CANALI INTERNI

ASM ha previsto[3], in conformità al Decreto Whistleblowing, la predisposizione di canali interni dedicati alle Segnalazioni per consentire a tutti i Segnalanti la possibilità di effettuare Segnalazioni relative a quanto previsto al Par. 6.3.

La Società, in conformità a quanto previsto dal Decreto Whistleblowing, prevede i seguenti canali di segnalazione interna che consentono ai Segnalanti di eseguire la Segnalazione mediante:

i. piattaforma informatica dedicata al Whistleblowing, accessibile al seguente link Whistleblowing (asmterni.it). - https://www.asmterni.it/trasparenza-prevenzione-della-corruzione-segnalazione-whistleblowing/

ii. canale orale che consente di mandare un messaggio vocale tramite la piattaforma informatica di cui al punto i. al seguente link: Whistleblowing (asmterni.it). - https://www.asmterni.it/trasparenza-prevenzione-della-corruzione-segnalazione-whistleblowing/

iii. su richiesta del Segnalante - avanzata mediante uno dei canali sopra dedicati - mediante incontro diretto fissato entro un termine ragionevole.

6.1.2. LA GESTIONE DELLA SEGNALAZIONE TRAMITE I CANALI INTERNI

La gestione dei canali interni della Società e delle Segnalazioni è affidata all'Organismo di Vigilanza. Qualora la Segnalazione riguardi uno o due membri dell'Organismo di Vigilanza, la gestione della stessa è affidata al membro/membri dell'OdV non coinvolti.

Qualora, invece, la Segnalazione riguardi tutti i membri dell'Organismo di Vigilanza, deve essere effettuata mediante il canale esterno gestito direttamente da ANAC, secondo quanto previsto al Par. 6.1.4. (in particolare, si rinvia al punto iii, lett. a).

La Società, nell'affidare la gestione delle Segnalazioni all'Organo Ricevente, ai sensi della normativa in materia di tutela dei dati personali, ha provveduto a disciplinare il rapporto con i membri esterni dell'Organo Ricevente quali responsabili del trattamento, ai sensi dell'art. 28 GDPR.

[3] Sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015.

Nel caso in cui dovesse essere nominato quale componente dell'Organo Ricevente un dipendente della Società (membro interno), questo dovrà essere autorizzato al trattamento dei dati personali, fornendogli istruzioni operative specifiche limitate al trattamento in esame.

Inoltre, la Società, ha stipulato un accordo ex art. 28 GDPR con il **fornitore della piattaforma** informatica che viene utilizzata, tra l'altro, per l'archiviazione della documentazione, come meglio precisato anche al Par. 6.5.

I canali interni sono progettati in modo da consentire un accesso selettivo alle Segnalazioni solo da parte dei predetti soggetti. Infatti il numero di persone responsabili della gestione delle Segnalazioni è limitato all'Organo Ricevente ed è soggetto all'obbligo di riservatezza.

I suddetti canali di segnalazione interna garantiscono la riservatezza del Segnalante, del Facilitatore e degli ulteriori soggetti sopra menzionati al Par. 4, della persona coinvolta o comunque dei soggetti menzionati nella Segnalazione.

La riservatezza è garantita anche con riguardo al contenuto della Segnalazione e della relativa documentazione. La protezione riguarda non solo il nominativo del Segnalante ma anche tutti gli elementi della Segnalazione dai quali si possa ricavare, anche indirettamente, l'identificazione del Segnalante.

L'identità del Segnalante e qualsiasi altra informazione da cui può evincersi - direttamente o indirettamente - tale identità non possono essere rivelate - salvo i casi espressamente previsti per legge - **senza il consenso espresso** del Segnalante stesso[4], a persone diverse dall'Organo Ricevente, competente a ricevere e a dare seguito alle Segnalazioni.

La riservatezza delle informazioni è garantita in ogni fase della Segnalazione, sia durante la fase di presa in carico e analisi preliminare, sia nel corso dell'indagine vera e propria, sia nella fase di valutazione finale e archiviazione della documentazione.

In particolare, le informazioni non vengono rivelate a persone diverse da quelle competenti a ricevere o a dare seguito alle Segnalazioni che sono formate in materia.

La documentazione in formato cartaceo è limitata al minimo indispensabile ed archiviata e custodita in armadi e locali dotati di serrature di sicurezza, ad accesso limitato solo all'Organo Ricevente.

[4] Il consenso, in tal caso, sarà acquisito attraverso la piattaforma informatica o altro canale con il quale è stata inviata la Segnalazione.

Quanto al canale interno della piattaforma informatica di cui al punto i. e ii., Par. 6.1.1:

- protegge l'identità della persona Segnalante, delle persone coinvolte e menzionate nella Segnalazione, nonché il contenuto della Segnalazione, mediante un sistema di crittografia. Gli strumenti di crittografia consentono la protezione dell'identità tramite l'utilizzo di un protocollo di crittografia garantendo così la protezione dei dati identificativi dell'identità del Segnalante. Inoltre, a seguito della segnalazione tramite la piattaforma, si genera un codice identificativo univoco che viene registrato sulla piattaforma che consente all'Organo Ricevente di dialogare con il Segnalante in modo "impersonale[5]";

- garantisce la possibilità di fornire aggiornamenti e indirizzare comunicazioni al Segnalante in merito alla Segnalazione (ad es. chiedere al Segnalante ulteriori elementi, fornire motivazioni in merito alla presentazione di una Segnalazione, aggiornare sullo stato di avanzamento delle indagini, ecc.);

- consente lo scambio di messaggi o documenti tra il Segnalante e l'Organo Ricevente durante l'indagine attraverso meccanismi interni della piattaforma che proteggono l'identità del Segnalante;

- garantisce la possibilità per il Segnalante di accedere alla Segnalazione effettuata e di verificare, in qualsiasi momento, lo stato di avanzamento delle indagini;

- garantisce la profilazione degli accessi da parte dei membri dell'Organo Ricevente;

- è ad accesso sicuro e protetto in quanto l'Organo Ricevente deve prima autenticarsi al pc con tecniche di autenticazione forte e poi fare altrettanto per accedere alla piattaforma;

- garantisce, ove possibile, il tracciamento dell'attività dell'Organo Ricevente nel rispetto delle garanzie a tutela del Segnalante, al fine di evitare l'uso improprio dei dati relativi alla Segnalazione e ciò, si precisa, evitando di tracciare qualunque informazione che possa ricondurre all'identità del Segnalante;

- garantisce che i log siano adeguatamente protetti da accessi non autorizzati e siano conservati per un periodo ragionevole rispetto alle finalità di tracciamento;

[5] Si precisa che spetta al Segnalante adottare tutte le misure necessarie per proteggere il codice univoco e la password per l'accesso alla piattaforma.

- non consente l'accesso ai dati personali da parte del fornitore della piattaforma, se non in casi particolari, disciplinati nell'accordo siglato con il Responsabile del Trattamento;

- laddove l'accesso alla piattaforma da parte dell'Organo Ricevente sia mediato da firewall o dispositivi proxy, viene garantita la non tracciabilità – sia sulla piattaforma informatica che negli apparati di rete eventualmente coinvolti nella trasmissione o monitoraggio delle comunicazioni - del Segnalante nel momento in cui viene stabilita la connessione;

- garantisce la presenza di misure tecniche per mantenere la sicurezza e l'impenetrabilità dei canali di comunicazione e trasmissione;

- garantisce la conservazione sicura della Segnalazione nonché la cancellazione della stessa dopo il periodo di conservazione determinato dal titolare del trattamento secondo quanto previsto dalla normativa di riferimento in materia;

- garantisce la possibilità di procedere alla cancellazione immediata in caso di raccolta accidentale di dati personali manifestamente non utili alla gestione di una specifica segnalazione.

Grazie all'utilizzo di queste misure di sicurezza che consentono di aumentare la tutela della riservatezza rispetto agli altri canali interni, **si raccomanda al Segnalante di utilizzare principalmente la piattaforma informatica di cui al punto i., Par. 6.1.1.**.

Laddove, invece, sia usato il sistema di messaggistica vocale con registrazione di cui al **canale illustrato al punto ii., Par. 6.1.1**, l'Organo Ricevente, previo consenso del Segnalante - rilasciato mediante l'utilizzo della funzionalità di messaggistica vocale dedicata nella piattaforma - documenta il contenuto della Segnalazione avvenuta con il sistema di messaggistica vocale mantenendo la registrazione della stessa sulla piattaforma, mediante sistema idoneo alla conservazione, all'ascolto nonché alla tutela della riservatezza, oppure mediante verbale che sarà archiviato nel rispetto della disciplina di riservatezza e di tutela dei dati personali, sulla piattaforma informatica.

Anche nell'ipotesi in cui la Segnalazione è effettuata oralmente nel corso di un incontro con l'Organo Ricevente, quest'ultimo, previo consenso del Segnalante, documenta il contenuto mediante registrazione su un dispositivo idoneo alla conservazione, all'ascolto nonché alla tutela della riservatezza oppure mediante verbale che sarà archiviato nel rispetto della disciplina di riservatezza e di tutela dei dati personali, sulla piattaforma informatica.

Laddove la Segnalazione sia effettuata in forma anonima - in quanto non viene fornita l'identità - la Società tratterà la stessa, ove circostanziata, come segnalazione ordinaria, come disciplinato al paragrafo 6.1.3, salvo

che successivamente sia integrata la Segnalazione con le generalità del Segnalante ai fini di acquisire le eventuali tutele di cui al Decreto Whistleblowing.

Ai sensi di quanto previsto dal Decreto Whistleblowing, quale corollario della tutela della riservatezza del Segnalante, si precisa che la Segnalazione e la documentazione allegata sono sottratte al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della L. n. 241/1990 nonché dal diritto di accesso civico generalizzato ex art. 5 del D.Lgs. n. 33/2013.

Per quanto attiene gli ulteriori aspetti relativi alla riservatezza si rinvia al seguente Par. 6.4.1..

La Società, nell'ottica di assicurare un'efficiente e tempestiva gestione della Segnalazione, segue il seguente *iter*.

Ricevuta la Segnalazione dall'Organo Ricevente, il Segnalante riceve un avviso di ricevimento della Segnalazione **entro sette giorni dalla data di ricezione**.

L'Organo Ricevente, nel rispetto delle tempistiche ragionevoli e della riservatezza dei dati, effettua un'analisi preliminare volta a verificare la sussistenza dei requisiti essenziali della Segnalazione per l'ammissibilità della stessa e poter accordare al Segnalante le tutele previste.

Ove quanto segnalato non sia adeguatamente circostanziato o si rendano necessari approfondimenti o chiarimenti, l'Organo Ricevente può chiedere elementi integrativi o documentazione al Segnalante tramite il canale a ciò dedicato, o anche di persona e/o telefonicamente e/o in videoconferenza.

Effettuata l'analisi preliminare, se la Segnalazione ha i requisiti essenziali per poter avviare l'attività istruttoria, l'Organo Ricevente procede con la fase di indagine vera e propria acquisendo tutti gli elementi probatori necessari per concludere l'istruttoria e valutare i fatti oggetto di Segnalazione, potendo svolgere dunque a titolo esemplificativo e non esaustivo, audizioni, acquisizioni documentali, anche informatiche, conferire incarichi a consulenti tecnici, ecc.. Di tutte le attività istruttorie suddette, l'Organo Ricevente cura l'adeguata verbalizzazione, tracciabilità e conservazione.

Qualora ne ravvisi la necessità, l'Organo Ricevente può avvalersi del supporto operativo della Funzione Internal Audit, ove esistente, e di consulenti terzi appositamente incaricati e ciò, nel rispetto del diritto alla riservatezza nonché della tutela dei dati personali ai sensi del GDPR e del Codice Privacy.

All'esito dell'istruttoria, laddove la Segnalazione sia ritenuta dall'Organo Ricevente:

a) fondata, quest'ultimo provvede immediatamente ad informare il Consiglio di Amministrazione della Società - nel rispetto del principio di riservatezza – che definirà le azioni da intraprendere, su proposta dell'Organo Ricevente, quali ad esempio l'irrogazione dei provvedimenti opportuni nel rispetto del sistema disciplinare adottato dalla Società nonché di quanto previsto dal contratto collettivo nazionale del lavoro applicabile (si rinvia, tra l'altro, al paragrafo 6 del Modello);
b) irrilevante ai sensi del Decreto Whistleblowing, quest'ultimo provvede ad informare il Consiglio di Amministrazione della Società mediante il flusso informativo annuale, salvo il caso in cui valuti la necessità di dover segnalarla immediatamente per motivi di urgenza o rilevanza e ciò sempre nel rispetto delle norme applicabili.

In ogni caso l'Organo Ricevente fornisce un riscontro[6] al Segnalante **entro tre mesi decorrenti dalla data dell'avviso di ricevimento o, in assenza dell'avviso, entro tre mesi dalla scadenza del termine di sette giorni dalla presentazione della Segnalazione**, dando conto delle misure previste o adottate o da adottare per dare seguito alla Segnalazione e dei motivi della scelta effettuata.

Laddove la Segnalazione afferisca uno o più membri del Consiglio di Amministrazione e questa risulti fondata, l'Organo Ricevente dovrà darne immediata comunicazione all'Assemblea dei Soci affinché adotti i provvedimenti del caso.

Laddove la Segnalazione pervenga erroneamente ad un soggetto non competente oppure attraverso un canale diverso da quelli specificamente previsti dalla presente Policy, la Segnalazione deve essere trasmessa **entro sette giorni dal suo ricevimento** all'Organo Ricevente, dando contestuale notizia della trasmissione al Segnalante.

6.1.3. GESTIONE SEGNALAZIONI ANONIME

Laddove la Segnalazione sia effettuata in forma anonima - in quanto non viene fornita l'identità - la Società tratterà la stessa ove circostanziata come segnalazione ordinaria, salvo che successivamente sia integrata la Segnalazione con le generalità del Segnalante ai fini di acquisire le eventuali tutele di cui al Decreto Whistleblowing.

[6] Il riscontro può ad esempio consistere nella comunicazione dell'archiviazione della procedura per mancanza di prove sufficienti o altri motivi, l'avvio di un'inchiesta interna ed eventualmente le relative risultanze e i provvedimenti adottati o il rinvio a un'Autorità competente per ulteriori indagini, nella misura in cui tali informazioni non pregiudichino l'inchiesta interna o l'indagine né ledano i diritti della persona coinvolta.
Tale riscontro è fondamentale per aumentare la fiducia nell'efficacia di tutto il sistema di protezione del whistleblower e ridurre il rischio di segnalazioni inutili.

In particolare, l'Organo Ricevente, prende in carico la segnalazione anonima circostanziata e verifica se risulti o meno fondata e rilevante sulla base degli elementi e circostanze oggetto della Segnalazione utili per la ricostruzione e l'accertamento di illeciti a vario titolo rilevanti.

L'iter di gestione della segnalazione anonima circostanziata è il medesimo di quanto illustrato al Par. 6.1.2. anche per quanto riguarda la fine dell'istruttoria e delle azioni conseguenti.

In caso di segnalazione anonima ASM provvede a registrarla e conservare la relativa documentazione non oltre cinque anni decorrenti dalla data di ricezione di tale segnalazione, rendendo così possibile rintracciarla nel caso in cui il Segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito misure ritorsive a causa di quella Segnalazione o denuncia anonima.

6.1.4. CANALE ESTERNO

Fermo restando il carattere principale dei canali interni sopra illustrati, i Segnalanti possono effettuare la Segnalazione attraverso il canale esterno che viene gestito direttamente da ANAC, rinvenibile al seguente link: Whistleblowing - www.anticorruzione.it

In particolare, il Segnalante può effettuare una Segnalazione tramite il canale esterno **solo nei seguenti casi,** come previsti dal Decreto Whistleblowing:

i. se, al momento della Segnalazione, i canali interni della Società non sono attivi o, anche se attivati, non sono conformi a quanto previsto dal Decreto Whistleblowing;

ii. se il Segnalante non ha avuto riscontro da parte dell'Organo Ricevente, dopo aver presentato la Segnalazione mediante canali interni (a titolo esemplificativo i canali interni non hanno funzionato correttamente, nel senso che la segnalazione non è stata trattata entro un termine ragionevole, oppure non è stata intrapresa un'azione per affrontare la violazione);

iii. se il Segnalante ha fondati motivi di ritenere, sulla base di circostanze concrete **allegate** ed informazioni **acquisibili** e, quindi, non su semplici illazioni, che:

   a) se effettuasse una Segnalazione mediante i canali interni, alla stessa non sarebbe dato efficace seguito (ciò si verifica quando, ad esempio, il responsabile ultimo nel contesto lavorativo sia coinvolto nella violazione, o se vi sia il rischio che la violazione o le relative prove possano essere occultate o distrutte, ecc.);

b) se effettuasse una segnalazione mediante i canali interni potrebbe sorgere il rischio di Ritorsione;

iv. se il Segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo imminente o palese per il pubblico interesse (si pensi, ad esempio, al caso in cui la violazione richieda un intervento urgente, per salvaguardare la salute e la sicurezza delle persone o per proteggere l'ambiente).

6.1.5. DIVULGAZIONE PUBBLICA

Ferma restando la preferenza per i canali interni di cui ai Par. 6.1.1. e, in via residuale, per il canale esterno nei casi previsti dal Decreto Whistleblowing di cui al Par. 6.1.4., al verificarsi delle condizioni di seguito indicate, il Segnalante può eseguire la Segnalazione mediante Divulgazione Pubblica, rendendo così di pubblico dominio le informazioni sulla violazione mediante ad esempio, la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone[7]:

i. una segnalazione mediante i canali interni non ha ricevuto riscontro nei termini previsti e ad essa ha fatto seguito una segnalazione esterna ad ANAC la quale, a sua volta, non ha fornito riscontro al segnalante entro termini ragionevoli;

ii. il Segnalante ha effettuato direttamente una segnalazione esterna all'ANAC la quale, tuttavia, non ha dato riscontro in merito alle misure previste o adottate per dare seguito alla segnalazione entro termini ragionevoli;

iii. il Segnalante sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze del caso concreto, ritiene che la violazione possa rappresentare un pericolo imminente o palese per il pubblico interesse (ad esempio una situazione di emergenza o al rischio di danno irreversibile, anche all'incolumità fisica di una o più persone, che richiedono che la violazione sia svelata prontamente e abbia un'ampia risonanza per impedirne gli effetti);

iv. il Segnalante sulla base di motivazioni ragionevoli e fondate alla luce delle circostanze del caso concreto ritiene che la segnalazione mediante canale esterno possa comportare il rischio di ritorsioni oppure possa non avere efficace seguito perché, ad esempio, teme che possano essere

[7] Il legislatore tiene naturalmente conto dell'evoluzione dei mezzi di diffusione di massa includendovi anche i social network e i nuovi canali di comunicazione (ad esempio facebook, twitter, youtube, instagram) che costituiscono uno strumento rapido e interattivo di trasmissione e veicolazione di informazioni e scambi tra reti di persone e organizzazioni.

occultate o distrutte prove oppure che chi ha ricevuto la Segnalazione possa essere colluso con l'autore della violazione o coinvolto nella violazione stessa (si consideri, a titolo esemplificativo, il caso in cui chi riceve la segnalazione di una violazione, accordandosi con la persona coinvolta nella violazione stessa, proceda ad archiviare detta segnalazione in assenza dei presupposti).

6.2. DENUNCIA ALL'AUTORITÀ GIURISDIZIONALE

Si precisa che, come previsto dal Decreto Whistleblowing, è riconosciuto ai soggetti di cui al Par. 4 anche la possibilità di valutare di rivolgersi alle Autorità Nazionali competenti, giudiziarie e contabili, per inoltrare una denuncia di condotte illecite di cui questi siano venuti a conoscenza in un contesto lavorativo pubblico o privato, quali ad esempio, l'Autorità Giudiziaria, la Polizia, Carabinieri, Guardia di Finanza, altre Forze di Polizia.

6.3. I CONTENUTI DELLA SEGNALAZIONE

La Segnalazione può avere ad oggetto:

i. **illeciti amministrativi, contabili, civili o penali**;

ii. **condotte illecite rilevanti ai sensi del Decreto 231 e violazioni del Modello della Società** (Parte Generale, Parte Speciale e Codice Etico);

iii. **illeciti commessi in violazione della normativa dell'UE indicata nell'Allegato 1 al Decreto Whistleblowing e di tutte le disposizioni nazionali che ne danno attuazione** (anche se queste ultime non sono espressamente elencate nel citato allegato). Le disposizioni normative contenute nell'Allegato 1 sono da intendersi come un riferimento dinamico in quanto vanno naturalmente adeguate al variare della normativa stessa. Con riferimento agli illeciti si riportano quelli relativi ai seguenti settori: contratti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;

iv. **atti od omissioni che ledono gli interessi finanziari dell'Unione Europea** (art. 325 del TFUE lotta contro la frode e le attività illegali che ledono gli interessi finanziari dell'UE) come

individuati nei regolamenti, direttive, decisioni, raccomandazioni e pareri dell'UE. Si pensi, ad esempio, alle frodi, alla corruzione e a qualsiasi altra attività illegale connessa alle spese dell'Unione;

v. **atti od omissioni riguardanti il mercato interno, che compromettono la libera circolazione delle merci, delle persone, dei servizi e dei capitali** (art. 26, paragrafo 2, del TFUE). Sono ricomprese le violazioni delle norme dell'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 vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;

vi. **atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea** nei settori indicati nei punti precedenti. In tale ambito vanno ricondotte, ad esempio, le pratiche abusive quali definite dalla giurisprudenza della Corte di Giustizia dell'Unione europea.

Le informazioni possono riguardare sia le violazioni commesse sia quelle non ancora commesse che il Segnalante, ragionevolmente, ritiene potrebbero esserlo sulla base di elementi concreti.

Possono essere oggetto di Segnalazione anche quegli elementi che riguardano condotte volte ad occultare le violazioni. Si pensi, ad esempio, all'occultamento o alla distruzione di prove circa la commissione della violazione.

È necessario che la Segnalazione sia il più possibile **circostanziata**, in particolare devono essere chiare:

i. le **circostanze di tempo e di luogo** in cui si è verificato il fatto oggetto della Segnalazione;

ii. la **descrizione del fatto**;

iii. **le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati**.

È possibile allegare documenti che possano fornire elementi di fondatezza dei fatti oggetto di Segnalazione, nonché l'indicazione di altri soggetti potenzialmente a conoscenza dei fatti.

Non possono essere oggetto di Segnalazione:

i. le notizie palesemente **prive di fondamento**;

ii. le informazioni che sono già totalmente di **dominio pubblico**;

iii. le informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. **voci di corridoio**);

iv. **le contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale** del Segnalante che attengono esclusivamente ai propri rapporti individuali di lavoro, ovvero inerenti ai propri rapporti di lavoro con le figure gerarchicamente sovraordinate;

v. **le segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali** indicati nella parte II dell'allegato al Decreto Whistleblowing ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al Decreto Whistleblowing. Tale circostanza attiene al settore dei servizi finanziari in cui da tempo l'Unione Europea ha esteso il valore della protezione delle persone segnalanti con l'obbligo di attivare canali di segnalazione interna ed esterna ponendo altresì il divieto esplicito di ritorsioni;

vi. **le segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale**, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione Europea. Sono escluse quindi le Segnalazioni che attengono agli appalti previsti agli artt. 15 e 24 delle direttive 2435 e 2536 del 2014 nonché all'art. 13 della direttiva del 2009/8137 e che sono esclusi anche dall'ambito di applicazione del Codice Appalti.

Si precisa che non è pregiudicata l'applicazione di alcune disposizioni nazionali o dell'Unione Europea in materia di:

i. **informazioni classificate:** le classifiche di segretezza, disciplinate nel nostro ordinamento dall'art. 42 della legge n. 124/2007, sono apposte dalle singole amministrazioni per circoscrivere la conoscenza delle informazioni per i soggetti che abbiano necessità di accedervi o a ciò abilitati, in ragione delle loro funzioni istituzionali;

ii. **segreto professionale forense:** con riferimento alla riservatezza delle comunicazioni tra gli avvocati e i loro clienti («segreto professionale forense») prevista dal diritto dell'Unione e dal diritto nazionale;

iii. **segreto professionale medico:** con riferimento all'obbligo di mantenere la natura riservata delle comunicazioni tra prestatori di assistenza sanitaria e i loro pazienti, nonché la riservatezza delle cartelle cliniche («riservatezza medica»);

iv. **segretezza delle deliberazioni degli organi giurisdizionali**;

v. **norme di procedura penale:** con riferimento all'obbligo della segretezza delle indagini ex art. 329 c.p.p.;

vi. **disposizioni sull'autonomia e indipendenza della magistratura, sulle funzioni e attribuzioni del Consiglio superiore della magistratura,** comprese le relative procedure, per tutto quanto attiene alla posizione giuridica degli appartenenti all'ordine giudiziario;

vii. **disposizioni in materia di difesa nazionale e di ordine e sicurezza pubblica** di cui al Regio decreto, 18 giugno 1931, n. 773, recante il testo unico delle leggi di pubblica sicurezza;

viii. **disposizioni in materia di esercizio del diritto dei lavoratori** di consultare i propri rappresentanti o i sindacati, di protezione contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, di autonomia delle parti sociali e del loro diritto di stipulare accordi collettivi, nonché di repressione delle condotte antisindacali di cui all'articolo 28 della legge 20 maggio 1970, n. 300.

6.4. LE TUTELE

6.4.1. L'OBBLIGO DI RISERVATEZZA

Oltra a quanto già descritto al Par. 6.1.2. che si richiama, le Segnalazioni non possono essere utilizzate oltre a quanto necessario per dare adeguato seguito alle stesse.

Per quanto riguarda i profili di tutela dei dati personali si rinvia al Par. 6.5.

Ove dovesse sorgere, all'esito della gestione della Segnalazione, un procedimento disciplinare, l'identità del Segnalante non può essere rivelata se la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla Segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia

fondata, in tutto o in parte, sulla Segnalazione e la conoscenza dell'identità del Segnalante sia indispensabile per la difesa dell'incolpato, la Segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso del Segnalante alla rivelazione della propria identità.

In tal caso è dato avviso al Segnalante - mediante comunicazione scritta - delle ragioni della rivelazione dei dati riservati, nonché nelle procedure di segnalazione interna ed esterna quando la rivelazione della identità del Segnalante e di qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità è indispensabile anche ai fini della difesa della persona coinvolta.

L'Organo Ricevente di ASM tutela l'identità delle persone coinvolte e delle persone menzionate nella Segnalazione fino alla conclusione dei procedimenti avviati in ragione della Segnalazione nel rispetto delle medesime garanzie previste in favore della persona Segnalante.

6.4.2. IL DIVIETO DI RITORSIONE

La tutela del Segnalante, del denunciante o di colui che esegue la Divulgazione Pubblica è garantita anche dal cosiddetto divieto di Ritorsione.

Tra le Ritorsioni si annoverano a titolo esemplificativo e non esaustivo:

i. licenziamento, sospensione o misure equivalenti;
ii. retrocessione di grado, mancata promozione, una valutazione della performance artatamente negativa;
iii. pretesa di risultati impossibili da raggiungere nei modi e nei tempi indicati;
iv. mutamento di funzioni, cambiamento del luogo di lavoro, riduzione dello stipendio, modifica dell'orario di lavoro;
v. ingiustificato mancato conferimento di incarichi con contestuale attribuzione ad altro soggetto;
vi. sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
vii. note di demerito o referenze negative;
viii. reiterato rigetto di richieste (ad es. ferie, congedi);
ix. revoca ingiustificata di incarichi;
x. sospensione ingiustificata di brevetti, licenze;
xi. adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
xii. coercizione, intimidazione, molestie o ostracismo;
xiii. discriminazione o comunque trattamento sfavorevole;

xiv. mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;

xv. mancato rinnovo o risoluzione anticipata di un contratto di lavoro a termine;

xvi. danni, anche alla reputazione della persona, in particolare sui social media, o pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;

xvii. inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;

xviii. conclusione anticipata o annullamento del contratto di fornitura di beni o servizi;

xix. annullamento di una licenza o di un permesso;

xx. richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Per godere della protezione prevista dal Decreto Whistleblowing con riferimento al divieto di misure ritorsive:

i. i Segnalanti, denuncianti o coloro che eseguono la Divulgazione Pubblica, devono ragionevolmente credere, anche alla luce delle circostanze del caso concreto e dei dati disponibili al momento della Segnalazione, Divulgazione Pubblica o denuncia, che le informazioni sulle violazioni segnalate, divulgate o denunciate siano veritiere[8] e pertinenti (cfr. Par. 6.3.);

ii. è necessario uno stretto collegamento tra la Segnalazione, denuncia, divulgazione e il comportamento, provvedimento, atto, omissione sfavorevole subito, direttamente o indirettamente, dalla persona Segnalante, denunciante o dal divulgatore.

La tutela prevista in caso di Ritorsioni non è garantita quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona Segnalante, denunciante, divulgatore per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'Autorità ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave. Nei casi di accertamento delle citate responsabilità, al soggetto Segnalante e denunciante sarà inoltre applicata una sanzione disciplinare.

[8] Non rileva invece, ai fini delle tutele, la circostanza che il soggetto abbia segnalato, effettuato divulgazioni pubbliche o denunce pur non essendo certo dell'effettivo accadimento dei fatti segnalati o denunciati e/o dell'identità dell'autore degli stessi o riportando anche fatti inesatti per via di un errore genuino.

È applicabile, se pur tardivamente, la protezione del Segnalante, denunciante o di chi effettua la Divulgazione Pubblica, per le Ritorsioni subite, qualora la sentenza di primo grado, sfavorevole per il Segnalante o denunciante, non venga confermata nei successivi gradi di giudizio.

Analogamente, l'instaurazione di un processo penale per i reati di diffamazione o di calunnia, in seguito alla Segnalazione, Divulgazione Pubblica o denuncia, concluso poi con archiviazione, non esclude l'applicazione di tale tutela in favore del Segnalante o denunciante.

6.4.3. LA PROTEZIONE IN CASO DI RITORSIONI

La **comunicazione di una Ritorsione** deve essere segnalata direttamente ed **esclusivamente** ad ANAC - soggetto competente per la gestione della stessa - al seguente canale: Whistleblowing - www.anticorruzione.it

Il soggetto tutelato, pertanto, **non dovrà utilizzare i canali interni** adottati dalla Società in caso di lamentata Ritorsione. Laddove la Società riceva una comunicazione di misure ritorsive per la quale non è competente, è tenuto a trasferirla ad ANAC entro 7 giorni inserendola nella piattaforma informatica di ANAC.

ANAC può avvalersi, per quanto di rispettiva competenza, della collaborazione dell'Ispettorato nazionale del lavoro.

È necessario che il soggetto tutelato fornisca ad ANAC elementi oggettivi dai quali sia possibile dedurre la consequenzialità tra Segnalazione, denuncia, Divulgazione Pubblica effettuata e la lamentata Ritorsione.

Nei casi di Ritorsioni tentate o minacciate, il soggetto tutelato, nel comunicare ad ANAC la Ritorsione subita, deve necessariamente fornire elementi da cui si possa evincere l'effettività della minaccia o del tentativo ritorsivo[9].

Sarà onere del soggetto che ha posto in essere condotte o atti ritorsivi provare di non aver posto una Ritorsione. Tale inversione dell'onere della prova sussiste solo in favore del Segnalante e non anche dei soggetti indicati al Par. 4 a cui sono estese le forme di tutela.

[9] Anche in caso di domanda risarcitoria all'Autorità giudiziaria la persona deve solo dimostrare di aver effettuato una Segnalazione, denuncia o Divulgazione Pubblica e di aver subito un danno. Salvo prova contraria, il danno si presume derivato dalla Segnalazione, denuncia, Divulgazione Pubblica.

Qualora tali soggetti lamentino di aver subito ritorsioni o un danno, incombe dunque in capo a loro l'onere probatorio.

Nel caso in cui l'Autorità accerti la natura ritorsiva di atti, provvedimenti, comportamenti, omissioni adottati, o anche solo tentati o minacciati, consegue la loro nullità e l'applicazione della sanzione amministrativa pecuniaria da 10.000 a 50.000 euro in capo all'ente.

L'Autorità considera responsabile della misura ritorsiva il soggetto che ha adottato il provvedimento/atto ritorsivo o comunque il soggetto a cui è imputabile il comportamento e/o l'omissione.

La responsabilità si configura anche in capo a colui che ha suggerito o proposto l'adozione di una qualsiasi forma di Ritorsione.

6.4.4. ULTERIORI MISURE A FAVORE DEI SEGNALANTI

Oltre alle tutele riconosciute al Segnalante, denunciante o a chi effettua una Divulgazione Pubblica di cui al Par. 6.4., per questi soggetti vi sono limitazioni di responsabilità in caso di rivelazione e diffusione di alcune categorie di informazioni[10], al ricorrere delle seguenti condizioni:

i. al momento della rivelazione o diffusione vi siano fondati motivi per ritenere che le informazioni siano necessarie per far scoprire la violazione;

ii. la Segnalazione, la Divulgazione Pubblica o la denuncia sia stata effettuata nel rispetto delle condizioni previste dal Decreto Whistleblowing per beneficiare delle tutele.

Inoltre, i Segnalanti possono beneficiare di **ulteriori misure di sostegno**, quali ad esempio, informazioni, assistenza e consulenze a titolo gratuito sulle modalità di Segnalazione e sulla protezione dalle Ritorsioni, nonché sulle modalità e condizioni di accesso al patrocinio a spese dello Stato. Per tali misure di sostegno si può consultare l'elenco degli enti del terzo settore istituito presso ANAC consultabile sul sito di quest'ultima.

6.5. PROTEZIONE DATI PERSONALI

Come premesso, il trattamento di dati personali relativi alle Segnalazioni è effettuato da ASM, in qualità di titolare del trattamento, nel rispetto dei princìpi europei e nazionali in materia di protezione di dati personali.

[10] Trattasi di informazioni coperte da segreto d'ufficio (art. 326 c.p.); segreto professionale (art. 622 c.p.); segreti scientifici e industriali (art. 623 c.p.); violazione del dovere di fedeltà e di lealtà (art. 2105 c.c.).

In particolare, ASM, quale titolare del trattamento, ad integrazione di quanto già illustrato al Par. 6.1.2. e 6.4.1., ha provveduto a:

- eseguire una **valutazione d'impatto sulla protezione dei dati personali** con riguardo al trattamento dei dati personali relativi alla Segnalazione di whistleblowing, supportato dal fornitore della piattaforma, incaricato ai sensi dell'art. 28 del GDPR quale responsabile del trattamento;
- fornire idonee **informazioni** alle persone Segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del GDPR;
- garantire l'**accesso selettivo** ai dati della Segnalazione solo all'**Organo Ricevente**;
- autorizzare, ove esistente, il **membro interno** dell'Organo Ricevente al trattamento dei dati personali, fornendogli istruzioni operative specifiche limitate al trattamento in esame;
- disciplinare il rapporto con i **membri esterni** dell'Organo Ricevente quali responsabili del trattamento, ai sensi dell'art. 28 GDPR;
- mantenere aggiornato il **registro dei trattamenti** con riguardo ai trattamenti dei dati personali connessi alla gestione delle segnalazioni whistleblowing;
- individuare **misure tecniche e organizzative** idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, adottando quindi misure appropriate a tutela dei diritti e delle libertà degli interessati;
- **disciplinare il rapporto con il fornitore della piattaforma informatica** ai sensi dell'Art. 28 del GDPR determinando le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali;
- erogare **sessioni formative** in materia sia al personale della Società che consentono la sensibilizzazione sulle tematiche di cui al Decreto Whistleblowing (con focus particolare sulle modalità di trattamento delle Segnalazioni, condizioni di segnalazione, ecc.), sia, ove fosse necessario, a coloro che rivestono il ruolo di Organo Ricevente;
- assicurare la separazione dell'oggetto della Segnalazione dalle informazioni che consentono l'identificazione del Segnalante (es. la possibilità di oscurare i dati personali, soprattutto quelli relativi al Segnalante, qualora, per motivi investigativi, altri soggetti debbano essere messi a conoscenza del contenuto della Segnalazione e/o della documentazione ad essa allegata);
- garantire la possibilità di attuare un sistema che consenta la **raccolta del consenso** del Segnalante alla divulgazione dell'identità – sia mediante il canale della piattaforma sia mediante gli altri canali interni - ad esempio, ove ciò sia necessario nell'ambito del procedimento disciplinare avviato dall'ente nei confronti del presunto autore della condotta segnalata;

- disciplinare la **gestione dei diritti** di cui agli articoli da 15 a 22 del GDPR nei limiti di quanto previsto dall'articolo 2-*undecies* del Codice Privacy[11].

  Laddove sussista il rischio che dall'esercizio dei diritti riconosciuti all'interessato nel Capo III del GDPR possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del Segnalante e che si possa compromettere la capacità di verificare efficacemente la fondatezza della Segnalazione o di raccogliere le prove necessarie, il Titolare del trattamento si riserva la facoltà di limitare o ritardare l'esercizio di detti diritti, conformemente a quanto stabilito dalle applicabili disposizioni di legge. In nessuna circostanza il Segnalato, o terzi soggetti, potranno esercitare i propri diritti di accesso per ottenere informazioni sull'identità del Segnalante, salvo che quest'ultimo abbia effettuato una Segnalazione Illecita.

Quanto alla conservazione della documentazione inerente alle Segnalazioni, ASM:

- conserva le Segnalazioni e la relativa documentazione sulla **piattaforma informatica** per il tempo necessario al trattamento della Segnalazione e comunque **non oltre 5 anni** a decorrere dalla data della comunicazione dell'**esito finale della procedura di segnalazione** - nel rispetto degli obblighi di riservatezza di cui alla normativa europea e nazionale in materia di protezione di dati personal (articolo 12 del Decreto Whistleblowing ed articolo 5, paragrafo 1, lettera e), GDPR) - salvo il caso in cui, durante il periodo di 5 anni dovesse sorgere un procedimento giudiziario derivante dalla Segnalazione; in tal caso il periodo di conservazione dei dati seguirà il percorso di detto procedimento giudiziario;

[11] **I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto**: a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; b) agli interessi tutelati in base alle disposizioni in materia di sostegno alle vittime di richieste estorsive; c) all'attività di Commissioni parlamentari d'inchiesta istituite ai sensi dell'articolo 82 della Costituzione; d) alle attività svolte da un soggetto pubblico, diverso dagli enti pubblici economici, in base ad espressa disposizione di legge, per esclusive finalità inerenti alla politica monetaria e valutaria, al sistema dei pagamenti, al controllo degli intermediari e dei mercati creditizi e finanziari, nonché alla tutela della loro stabilità; e) allo svolgimento delle investigazioni difensive o all'esercizio di un diritto in sede giudiziaria; f) **alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio**; f-bis) agli interessi tutelati in materia tributaria e allo svolgimento delle attività di prevenzione e contrasto all'evasione fiscale. (...)
3. Nei casi di cui al comma 1, lettere a), b), d) e), f) e f-bis) i diritti di cui al medesimo comma sono esercitati conformemente alle disposizioni di legge o di regolamento che regolano il settore, che devono almeno recare misure dirette a disciplinare gli ambiti di cui all'articolo 23, paragrafo 2, del Regolamento. **L'esercizio dei medesimi diritti può, in ogni caso, essere ritardato, limitato o escluso con comunicazione motivata e resa senza ritardo all'interessato, a meno che la comunicazione possa compromettere la finalità della limitazione, per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata, tenuto conto dei diritti fondamentali e dei legittimi interessi dell'interessato, al fine di salvaguardare gli interessi di cui al comma 1, lettere** a), b), d), e), **f)** e f-bis). In tali casi, i diritti dell'interessato possono essere esercitati anche tramite il Garante con le modalità di cui all'articolo 160. In tale ipotesi, il Garante informa l'interessato di aver eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. Il titolare del trattamento informa l'interessato delle facoltà di cui al presente comma.

- laddove sia usato per la Segnalazione il sistema di messaggistica vocale con registrazione di cui al canale illustrato al punto ii. Par. 6.1.1, l'Organo Ricevente, **previo consenso del Segnalante** - rilasciato mediante l'utilizzo della funzionalità di messaggistica vocale dedicata nella piattaforma - documenta il contenuto della Segnalazione avvenuta con il sistema di messaggistica vocale mantenendo la registrazione della stessa sulla piattaforma, mediante sistema idoneo alla conservazione, all'ascolto nonché alla tutela della riservatezza, oppure mediante verbale che sarà archiviato nel rispetto della disciplina di riservatezza e di tutela dei dati personali sulla piattaforma;
- quando, su richiesta del Segnalante, la Segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, **previo consenso del Segnalante**, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione, all'ascolto e alla tutela della riservatezza oppure mediante verbale che sarà archiviato nel rispetto della riservatezza e della tutela dei dati personali sulla piattaforma. In caso di verbale, la persona Segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione;
- in caso di segnalazione anonima, ASM provvede a registrarla e conservare la relativa documentazione **non oltre cinque anni decorrenti dalla data di ricezione di tale segnalazione anomima,** rendendo così possibile rintracciarla nel caso in cui il Segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito misure ritorsive a causa di quella Segnalazione o denuncia anonima.

6.6. SANZIONI DISCIPLINARI E ALTRI PROVVEDIMENTI

ASM prevede nel proprio sistema disciplinare sanzioni disciplinari anche in caso di accertamento:

- di Ritorsioni[12];
- di Segnalazione ostacolata o di tentativo di ostacolarla;
- di violazione dell'obbligo di riservatezza;
- di mancata istituzione dei canali di Segnalazione;

[12] La tutela prevista in caso di Ritorsioni non è garantita quando è accertata, anche con sentenza di primo grado, la responsabilità penale della persona Segnalante, denunciante, divulgatore per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'Autorità ovvero la sua responsabilità civile, per lo stesso titolo, nei casi di dolo o colpa grave. Nei casi di accertamento delle citate responsabilità, al soggetto Segnalante e denunciante sarà inoltre applicata una sanzione disciplinare.

- di mancata adozione di procedure per l'effettuazione e la gestione delle Segnalazioni ovvero di mancata conformità di tali procedure rispetto al Decreto Whistleblowing;

- mancato svolgimento dell'attività di verifica e analisi delle Segnalazioni ricevute;

- anche con sentenza di primo grado, della responsabilità civile della persona Segnalante per diffamazione o calunnia nei casi di dolo o colpa grave, salvo che la medesima sia stata già condannata, anche in primo grado, per i reati di diffamazione o di calunnia o comunque per i medesimi reati commessi con la denuncia all'Autorità competente.

Inoltre, laddove la Segnalazione risulti fondata e sia accertata la responsabilità del soggetto segnalato, si rinvia a quanto previsto al Par. 6.1.2.

Con riguardo alla disciplina del sistema disciplinare in essere, si rinvia al Modello 231 adottato da ASM per le sanzioni irrogabili (cfr. Par. 6 del Modello) nonché a quanto previsto dal contratto collettivo nazionale del lavoro applicabile e dalle altre norme nazionali applicabili.

6.7. OWNER DELLA POLICY E ARCHIVIAZIONE

L'Unità Legale è responsabile, per quanto di competenza, a mantenere aggiornata la presente Policy e a comunicare alle altre funzioni aziendali quanto necessario per diffonderla ogniqualvolta sia apportata una modifica.

L'Organo Ricevente assicura la tracciabilità dei dati e delle informazioni e provvedono alla conservazione e archiviazione della documentazione prodotta, cartacea e/o elettronica, in modo da consentire la ricostruzione delle diverse fasi del processo stesso, nel rispetto degli obblighi di riservatezza e della tutela dei dati personali.

6.8. ENTRATA IN VIGORE E MODIFICHE

La presente Policy assume validità dalla data di approvazione da parte del Consiglio di Amministrazione della Società.

Ogni modifica deve essere deliberata dal Consiglio di Amministrazione.