VALUTAZIONE D'IMPATTO

AI SENSI DELL'ART. 35 REGOLAMENTO UE 2016/679 (GDPR)

TRATTAMENTO O CATEGORIA DI TRATTAMENTO: **Gestione dei canali di segnalazione**
DESCRIZIONE DEL TRATTAMENTO[1]

- **Natura, finalità e contesto del trattamento:**

Il Decreto n. 24 del 15 marzo 2023 (di seguito anche "Decreto") è intervenuto riformando la disciplina del Whistleblowing prevedendo espressamente che la nuova normativa si applicasse ai soggetti del settore pubblico, comprese le società a controllo pubblico e in house, nonché ai soggetti del settore privato che hanno adottato un Modello Organizzativo ex D.Lgs. 231/01 anche se non hanno raggiunto la soglia dei 50 dipendenti.

Tale Decreto, infatti, ha modificato l'art. 6 del D. Lgs. 231/01 specificando che i Modelli ex D. Lgs. 231/01 prevedono ai sensi del Decreto i canali di segnalazione interna, il divieto di ritorsione e il sistema disciplinare.

Il nuovo sistema di segnalazione prevede l'operatività di tre diversi canali: i) un canale pubblico (al ricorrere dei presupposti di cui all'art. 15, la tutela è estesa anche a coloro che effettuano una cd. "divulgazione pubblica", cioè una segnalazione eseguita tramite mezzi di stampa o altri strumenti di comunicazione simili), ii) un canale esterno (il cui destinatario è stato individuato nell'ANAC) e iii) un canale interno.

Con riferimento al canale interno, il Decreto ribadisce che il canale deve garantire la piena riservatezza delle persone coinvolte (segnalante, segnalato, soggetti citati, etc.) nonché del contenuto della segnalazione, anche tramite il ricorso a strumenti di crittografia.

Sul punto, è poi precisato che la segnalazione può essere ricevuta in forma scritta, anche informatica, o in forma orale (i.e. tramite linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole).

Il Decreto prevede infine espressamente l'obbligo di mettere a disposizione dei potenziali segnalanti informazioni chiare sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni interne, nonché sul canale, sulle procedure e sui presupposti per effettuare le segnalazioni esterne.
In particolare, le informazioni dovranno essere rese facilmente visibili nei luoghi di lavoro e sul sito internet dell'ente (in una sezione dedicata).

- **Responsabilità legate al trattamento:**

Dott. Arturo Vallone Dirigente della S.R.R. Messina Area Metropolitana appartiene alla categoria dei soggetti del settore pubblico, nonché ha adottato il Modello di Organizzazione e di Gestione *ex* articolo 6 del D. Lgs. n. 231/2001 e pertanto ha dovuto adottare un sistema di gestione delle segnalazioni conforme alle prescrizioni del Decreto.

[1] La descrizione del trattamento viene operata sulla base della procedura whistleblowing adottata nell'ambito del MOG 231/01 e sulla base delle indicazioni fornite dal responsabile informatico e del RPCT.

La società è Titolare del trattamento dei dati personali legati alla segnalazione (dati del segnalante, delle persone coinvolte e gli ulteriori dati contenuti nella segnalazione ricevuta).

Il canale che permette di ricevere segnalazioni in forma scritta è rappresentato:

- **da una apposita sezione del sito sulla quale è possibile la compilazione di un *form* di segnalazione;**
- **da una piattaforma messa a disposizione dal fornitore ……, accessibile mediante un link sul sito della società. La piattaforma crea un *form* anonimo per l'invio successivo della segnalazione all'indirizzo di posta elettronica del gestore della segnalazione. Il fornitore viene debitamente nominato Responsabile del trattamento dal Titolare, nell'ambito della propria attività.**
- **dalla messa a disposizione della casella di posta elettronica dedicata whistleblowing@.....**

Il Gestore della Segnalazione interna è il RPCT.

Il Gestore della Segnalazione riceve formale incarico come soggetto gestore dei canali interni che comprende anche la lettera di designazione ad autorizzato ex artt. 29 Reg. UE 679/2016 (anche "GDPR") e 2-quaterdecies D. Lgs. n. 196/2003 (anche "Codice Privacy"). La lettera prevede specifiche istruzioni per il corretto trattamento dei dati personali di cui alla segnalazione, di cui la società è Titolare del trattamento ex art. 4 par. 1 n. 7) GDPR.

Il Gestore delle Segnalazioni può essere supportato da soggetti interni o esterni alla Società ma deve mantenere la riservatezza sull'identità del segnalante, a meno che questi non abbia fornito il consenso alla rivelazione della propria identità. Questi soggetti se interni sono autorizzati dai Titolari ai sensi dell'art. 29 GDPR e 2-quaterdecies D. Lgs. 196/2003, se esterni sono nominati Responsabili del trattamento ex art. 28 GDPR.

Allo stesso modo nel procedimento disciplinare a carico del segnalato, il Gestore della Segnalazione può riferire i dati del segnalante alla funzione competente solo se la segnalazione è l'unico elemento su cui si fonda il procedimento e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, a patto che il segnalante abbia fornito il consenso. I componenti della funzione competente sono autorizzati dal Titolare ai sensi dell'art. 29 GDPR e 2-quaterdecies D. Lgs. 196/2003.

- **Categorie di dati (personali e sensibili) oggetto di trattamento:**

I dati coinvolti nel trattamento sono astrattamente riconducibili a tutte le categorie di dati personali, anche alla categoria di dati particolari *ex* art. 9 GDPR e quella relativa a condanne e reati *ex* art. 10 GDPR.
In particolare, sono raccolti i seguenti dati:

a) **le generalità di chi effettua la segnalazione (ferma restando per il segnalante la possibilità di effettuare una segnalazione anonima);**
b) **la chiara e completa descrizione dei fatti oggetto di segnalazione e delle modalità con le quali se ne è avuta conoscenza;**
c) **il nominativo o altro dato che consenta di identificare le persone coinvolte;**
d) **informazioni relative ad eventuali documenti che possono confermare la fondatezza dei fatti riportati;**
e) **ogni altra informazione contenuta nelle segnalazioni o acquisita nell'ambito dell'istruttoria.**

Nelle ipotesi di segnalazioni tramite canale orale e quindi mediante incontro diretto, la voce del segnalante non verrà registrata e quindi non saranno trattati dati biometrici (voce segnalante), ma è prevista redazione di un verbale.

- **Soggetti interessati:**

I soggetti interessati del trattamento sono:

a) **la persona segnalante: la persona fisica che effettua la segnalazione sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;**
b) **il facilitatore: una persona fisica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;**

c) **gli altri soggetti di cui all'art. 3 co. 5 del D.lgs. 24/2023;**
d) **la persona coinvolta: la persona fisica menzionata nella segnalazione come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata.**

- **Descrizione del ciclo di vita del trattamento (raccolta, passaggi del trattamento, archiviazione, distruzione):**

Il Titolare ha previsto di istituire due canali di segnalazione interna che possono essere alternativamente utilizzati:
- **un canale scritto, informatico tramite piattaforma whistleblowing accessibile da qualsiasi browser (anche accedendo da dispositivi mobili) avente il seguente indirizzo: whistleblowing@srrmessinaareametropolitana.it che consente di inviare segnalazioni per iscritto. Questo strumento offre le più ampie garanzie di riservatezza per il segnalante. Ricevuta la segnalazione, il Gestore accede alla Piattaforma ed esamina il contenuto della segnalazione e gli eventuali documenti allegati.**

- **un canale orale, mediante un appuntamento fisico con il Gestore della Segnalazione entro 15 giorni dal primo contatto. Nel corso di questo incontro la segnalazione verrà raccolta dal Gestore e istruita.**

Tramite entrambi i suddetti canali è possibile prenotare un incontro da svolgersi di persona con il Gestore della segnalazione.

Il Gestore della Segnalazione conserva le informazioni indicate, oltre a tutti i documenti relativi all'istruttoria e i verbali degli incontri tenuti con il segnalante o persona coinvolta o testimoni su device personale.

- **Periodo di conservazione dei dati:**

Le segnalazioni saranno conservate per il tempo strettamente necessario alla gestione delle stesse e, in ogni caso, per un periodo massimo di cinque anni. La Piattaforma prevede una cancellazione automatica della segnalazione di volta in volta una volta inviata la mail al gestore della segnalazione.

Non è possibile per il Gestore della Segnalazione cancellare manualmente le segnalazioni senza lasciarne traccia sul server aziendale. Il responsabile IT non può entrare nell'account, modificare le credenziali, prendere lettura delle mail inviata/ricevute senza che il gestore della segnalazione non ne abbia conoscenza, in quanto il sistema prevede che ogni accesso da device diverso sia segnalato al gestore alla segnalazione.
Inoltre l'accesso da parte del gestore della segnalazione all'account su device diverso deve essere di volta in volta autorizzato anche dal responsabile IT.

Analogamente, l'eventuale documentazione utilizzata nel corso dell'istruttoria (registrazioni, verbali, documentazione raccolta etc.) sarà gestita da parte del Gestore della Segnalazione nel rispetto del termine di conservazione di cui sopra.

- **Possibili comunicazioni a terzi:**

I dati potranno essere comunicati a:
- **Autorità Giudiziarie e di pubblica sicurezza**
- **ANAC**
- **Soggetto incaricato della revisione legale**
- **Collegio sindacale (laddove istituito)**
- **OdV**
- **Enti Certificatori**
- **Eventuali altre PA se previsto da un obbligo di legge, in caso di richiesta esplicita.**

- **Modalità (cartacee e automatizzate) e strumenti con cui viene effettuato il trattamento:**

I dati sono raccolti esclusivamente mediante strumenti elettronici e per via telematica o connessione telefonica. Eccezionalmente in modalità cartacea.

- **Soggetti che potranno accedere ai dati unitamente alle finalità o alle motivazioni sottese all'accesso:**

Le informazioni contenute nella segnalazione sono accessibili solo al Gestore della Segnalazione.
Tale soggetto potrà riferire l'identità del segnalante nell'ambito dell'istruttoria solo laddove il segnalante abbia fornito espresso consenso.

Il Gestore della Segnalazione è autorizzato al trattamento ex art. 29 GDPR.

Tutti gli altri soggetti interni a cui è necessario riferire il contenuto della segnalazione per lo svolgimento dell'istruttoria o della successiva fase relativa al procedimento disciplinare sono soggetti autorizzati al trattamento.

In ogni caso in assenza di consenso del segnalante deve essere mantenuta la riservatezza sull'identità del segnalante, per cui non verranno trattati i suoi dati personali.

VALUTAZIONE SULLA NECESSARIETÀ DEL TRATTAMENTO
(liceità, necessità, proporzionalità)

- **Finalità determinate, esplicite e legittime:**
  a) **presa in carico della segnalazione da parte del Gestore della Segnalazione,**
  b) **invio di eventuali richieste e/o ricezione di riscontro alle richieste inviate dal segnalante e dal Gestore della Segnalazione,**
  c) **gestione istruttoria: esecuzione di verifiche sulla fondatezza della segnalazione,**
  d) **gestione dei provvedimenti conseguenti, anche sotto il profilo disciplinare.**

- **Impiego di dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità e le modalità con cui il titolare assicura l'accuratezza dei dati:**

Le attività di trattamento dei dati connesse alla gestione delle segnalazioni possono riguardare la commissione di reati o di atti contrari ai principi di cui alla normativa sopra richiamata, sono esclusivamente quelle pertinenti al perseguimento delle finalità già menzionate.
I dati contenuti nella segnalazione sono ricevuti dai soggetti autorizzati e trattati per il perseguimento delle finalità già menzionate, facendo ricorso ai mezzi prima descritti.
Le informazioni non rilevanti non saranno oggetto di ulteriore trattamento; saranno trattati, infatti, i soli dati ritenuti rilevanti per il proseguimento delle indagini interne che dovessero ritenersi necessarie.
Non sono raccolti, e se raccolti sono cancellati, dati che non sono strettamente necessari alla gestione della segnalazione.

- **Limitazione della conservazione ad un arco di tempo non superiore al conseguimento delle finalità:**

Come riportato anche nel Registro delle attività di trattamento di cui all'art. 30 GDPR, il Titolare, in ossequio al principio di limitazione della conservazione dei dati, ha previsto che i dati vengano conservati per un termine massimo di cinque anni dalla ricezione della segnalazione; solo in caso di contenzioso, i dati verranno conservati fino all'irrevocabilità/definitività dello stesso.

- **Presupposto di legittimità del trattamento (e.g. consenso, obbligo legale, legittimo interesse del titolare):**

La base giuridica dei trattamenti suindicati è rinvenibile nell'adempimento dell'obbligo legale ex art. 6, par. 1, lett. c) del GDPR come descritto nel D. Lgs. n. 24/2023.
La base giuridica è, altresì, rinvenibile, per ciò che riguarda il trattamento di categorie particolari di dati, nell'articolo 9, par. 2, lett. b) del GDPR in quanto il trattamento è necessario per assolvere agli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della

sicurezza sociale e protezione sociale, nonché nell'articolo 9, par. 2 lett. g) del GDPR in quanto il trattamento è necessario per motivi di interesse pubblico rilevante sulla base dell'art. 2-sexies del D. Lgs. n. 196/2003.

Il trattamento dei dati relativi a condanne e reati resosi eventualmente necessario per la gestione della segnalazione ricevuta è legittimo sulla base dell'art. 10 GDPR in correlazione con l'art. 2-octies del D. Lgs. n. 196/2003.

VALUTAZIONE SULLE MISURE TECNICHE E ORGANIZZATIVE ADOTTATE

- **Modalità attraverso le quali sono state fornite ai soggetti interessati informazioni chiare, complete e comprensibili circa il trattamento dei loro dati, in cui siano indicati in particolare i soggetti a cui possono rivolgersi per ottenere ulteriori informazioni ovvero per esercitare i propri diritti:**

L'informativa *ex* art. 13 GDPR è inserita nella piattaforma e l'invio della segnalazione costituisce *ex se* lettura e piena conoscenza della stessa prima dell'invio della segnalazione.

L'informativa inoltre è pubblicata nella pagina informativa del sito unitamente alla Procedura di Gestione delle Segnalazioni e alle altre informazioni sullo strumento di segnalazione.

- **Procedure elaborate per garantire il diritto e l'effettiva possibilità di procedere all'accesso, alla portabilità, alla cancellazione, alla rettifica e all'aggiornamento dei dati, nonché all'opposizione e alla limitazione del trattamento:**

L'esercizio dei diritti riferiti all'interessato è dettagliato nelle informative rese note come descritte al punto che precede, e quindi con le medesime modalità previste per la segnalazione.

Al fine di proteggere la riservatezza dell'identità del Segnalante, potrà essere preclusa la possibilità di esercitare i diritti previsti dagli artt. da 15 a 22 del Regolamento, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto alla riservatezza dell'identità del segnalante, ai sensi dell'art. 23, par. 1, lett. i) del Regolamento e dell'art. 2-undecies, co. 1, lett. f) del Codice Privacy.
Il segnalante potrà esercitare i diritti di cui agli artt. da 15 a 22 del Regolamento per il tramite dell'Autorità Garante, con le modalità di cui all'art. 160 del Codice Privacy.

- **In caso di trasferimenti all'estero, le garanzie che legittimano il trasferimento di dati verso un Paese terzo extra-europeo (e.g. decisioni di adeguatezza, clausole contrattuali standard):**

N/A (Il fornitore crea un *form* anonimo per l'invio successivo della segnalazione all'indirizzo di posta elettronica del gestore della segnalazione, ed in ogni caso i dati non vengono trattati al di fuori dell'UE o , se ciò avviene, sono state date apposite istruzioni al fornitore, in qualità di responsabile del trattamento, al riguardo.)

- **In caso di presenza di un responsabile esterno o di un co-titolare i rispettivi obblighi sono chiaramente individuati e disciplinati in un contratto o altro atto giuridico.**

Se il Titolare utilizza la Piattaforma di un fornitore terzo, in esito alla valutazione positiva, è stata sottoscritta la nomina *ex* art. 28 GDPR che costituisce appendice e parte integrante del contratto sottoscritto tra le parti.

- **Altre misure organizzative adottate:**

Il Gestore della Segnalazione ha ricevuto e sottoscritto apposita lettera di designazione al trattamento – *ex* artt. 29 GDPR e art. 2-*quaterdecies* D. Lgs. n. 196/2003, con cui il Titolare ha fornito specifiche istruzioni per il corretto trattamento dei dati derivante dallo svolgimento delle loro mansioni ed attribuzioni.

In particolare:

a) **l'accesso alla Piattaforma avviene con credenziali personali appositamente rilasciate dal fornitore al Gestore della Segnalazione, che avrà cura di custodirle, cambiare la password al primo accesso e non comunicarla a terzi.**
b) **eventuali informazioni aggiuntive raccolte nel corso di verifiche/indagini intraprese a seguito di una segnalazione dovranno essere archiviate dal Gestore delle segnalazioni in uno spazio di archiviazione protetto da PW o crittografia e consegnate al Titolare al termine del rapporto e quindi al venir meno della presente nomina. Eventuali documenti cartacei saranno scannerizzati e inseriti in tale archivio e l'originale sarà conservato a cura del Gestore.**
c) **Le segnalazioni potranno essere conservate fino a 5 anni a cura del Gestore della Segnalazione in Piattaforma e nello spazio di archiviazione suddetto. La cancellazione in Piattaforma sarà automatica una volta decorso il termine di 5 anni dalla data di ricezione della segnalazione. In ogni caso, il Gestore della Segnalazione avrà cura di verificare che il periodo di conservazione sopra definito sia rispettato.**
d) **nel caso in cui, nella presentazione della segnalazione e/o nelle successive integrazioni documentali, siano inserite delle informazioni non necessarie ai fini della gestione della segnalazione il Gestore della Segnalazione è tenuto alla cancellazione immediata;**

Il Titolare ha autorizzato gli altri soggetti interni potenzialmente coinvolti nelle segnalazioni e eroga, altresì, sessioni formative periodiche in materia di protezione dei dati personali.

In aggiunta, il Titolare ha adottato la Procedura di Gestione delle Segnalazioni.

- **Misure tecniche di sicurezza adottate:**

Il device personale del Gestore della segnalazione presso il quale saranno archiviati gli atti dell'istruttoria dispone almeno delle seguenti misure:

- **sistemi di autenticazione;**
- **utilizzo di password robuste;**
- **cambio password ogni 6 mesi;**
- **accesso al PC inibito a terzi;**
- **utilizzo di cartelle con password diversa da quella di accesso generale;**
- **modalità automatica di inserimento del blocco pc in caso di inattività prolungata, non superiore a 1 minuto;**
- **utilizzo di software aggiornati e regolarmente licenziati;**
- **sistema antivirus licenziato e costantemente aggiornato.**

IDENTIFICAZIONE, ANALISI E GESTIONE DEI RISCHI
PER I DIRITTI E LE LIBERTA' DEGLI INTERESSATI
(accessi illegittimi ai dati, modifica indesiderata dei dati, scomparsa dei dati)

- **Individuazione degli impatti potenziali per i diritti e le libertà degli interessati: (assegnare a ciascun rischio individuato un livello di probabilità di realizzazione e un grado di potenziale impatto e gravità):**

L'eventuale divulgazione/alterazione o perdita delle informazioni personali trattate dal Titolare può comportare un impatto sulla vita sociale e personale degli interessati, che può essere superato con difficoltà. Ad esempio, vi possono essere danni per la reputazione, discriminazione, furto di identità, dati fisici o psicologici, perdita di controllo dei dati, ricatto.

- **Identificazione delle possibili fonti di rischio: comportamenti di operatori o terzi (e.g. sottrazione credenziali, distrazione, comportamenti fraudolenti o sleali), eventi (e.g. sottrazione di strumenti che contengono dati, eventi distruttivi naturali o artificiali), ogni altra ipotesi di violazione dei dati personali (e.g. accessi non autorizzati, alterazione, perdita o distruzione dei dati): *cfr* tabella sottostante**
- **Gestione dei rischi (descrizione delle misure adottate, attraverso le quali il rischio può essere eliminato completamente, ovvero essere mitigato o, *in extremis*, accettato): *cfr* tabella sottostante**

MISURE SICUREZZA PIATTAFORMA WHISTLEBLOWING	
Tipologia di servizio e ubicazione Data Center:	Servizio di whistleblowing software basato su creazione di form anonimo inviato al Gestore della segnalazione. (Il fornitore della Piattaforma è ……) Il Data Center del fornitore …….. si trova **all'interno/esterno** dell'UE. La descrizione delle funzionalità della Piattaforma e delle misure di sicurezza adottate è rinvenibile al seguente link: ….....
Sistemi autenticazione per poter accedere alla piattaforma informatica aziendale:	Per l'accesso al sito è necessaria autenticazione semplice, con una serie di cautele. È prevista successivamente l'autenticazione a doppio fattore (c.d. *strong autentication*).
Meccanismi di profilazione degli utenti:	La procedura Whistleblowing garantisce l'accesso selettivo ai dati delle segnalazioni da parte dei soli soggetti che sono autorizzati al trattamento. In particolare, prevede l'accesso ai soli utenti registrati a sistema e che possono essere qualificati come Amministratori o Riceventi, e che hanno accesso rispettivamente alla sola amministrazione o alle sole segnalazioni.
Registrazione Log accesso: tracciamento delle operazioni svolte da parte del destinatario delle segnalazioni e da parte degli eventuali altri soggetti istruttori,	La procedura applica una politica "no-log" a partire dall'arrivo della connessione al Sistema del fornitore grazie alla quale non viene registrato l'indirizzo IP del segnalante. La procedura registra poi gli Audit-Log relativi agli accessi alla piattaforma degli utenti (Riceventi, Amministratori e Segnalante, che rimane anonimo) in modalità *privacy-preserving*. Sono ad esempio registrate le operazioni eseguite, la data e l'orario, il protocollo di connessione utilizzato, l'uso di un PC o di un cellulare per l'accesso.
Sistemi di protocollo di trasporto dati per l'accesso alla piattaforma da parte degli utenti **(tipo protocollo https), sia dal punto di vista della riservatezza che dal punto di vista dell'integrità dei dati relativi**	La Piattaforma utilizza protocollo Https che è configurato e mantenuto costantemente aggiornato dal fornitore. Per verificare la configurazione Https si possono utilizzare i seguenti strumenti, inserendo l'indirizzo della piattaforma: https://www.ssllabs.com/ssltest/analyze.html https://observatory.mozilla.org/ https://securityheaders.com/

all'identità del soggetto che ha effettuato la segnalazione e al contenuto della segnalazione stessa	
Monitoraggio segnalazione	Il segnalante non può monitorare lo stato della segnalazione e/o caricare ulteriore documentazione direttamente dalla piattaforma, ma soltanto rivolgersi al RPCT. Al termine della segnalazione, al segnalante allo stato non viene rilasciata nessuna ricevuta, ma è previsto il rilascio di un ticket/ricevuta mediante il quale potrà in seguito contattare il RPCT e monitorarne lo stato di avanzamento. Allo stesso tempo il ricevente instaura un colloquio diretto con il segnalante, mediante il quale è possibile richiedere, se del caso, ulteriori elementi di dettaglio o di supporto alla segnalazione stessa. Allo stesso modo il Ricevente può verificare se effettivamente il Segnalante ha fatto accesso e letto l'ultimo aggiornamento della Segnalazione. È prevista l'opzione che permette anche al Ricevente – con le medesime modalità - di caricare documentazione affinché il Segnalante (non anonimo) possa visionarla.

VALUTAZIONE DEL RISCHIO E PIANO DI AZIONE

Descrizione finale della valutazione del rischio:
Si riportano di seguito le valutazioni eseguite in merito ai rischi per i diritti e le libertà degli interessati, connessi al trattamento di cui trattasi.

Il trattamento dei dati connesso alla gestione delle segnalazioni *whistleblowing* è considerato ad elevato rischio per i diritti e le libertà interessati dal momento che potrebbe riguardare potenzialmente dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse (Allegato 1 al provvedimento n. 467 dell'11 ottobre 2018 del Garante per la protezione dei dati personali).

Partendo, dunque, da un rischio astratto elevato (R>9), sono state prese in considerazione le misure di sicurezza adottate dal Titolare per mitigare i rischi connessi al trattamento al fine di individuare così il rischio residuo.

La valutazione delle misure di sicurezza è stata effettuata sulla base dei criteri riportati nella tabella sottostante, i quali danno una corrispondenza in termini di 3 livelli di adeguatezza di tali misure:

Livello	Linee guida per la valutazione	Valutazione rischio residuo
1- Inadeguato	Il controllo non è previsto o è assente nella pratica.	Tale livello comporta il mantenimento della classe di rischio individuata per il rischio astratto.
2- Parzialmente adeguato	Le misure sono state adottate, tuttavia sono state rilevate delle mancanze che non ne	Tale livello comporta il passaggio ad una classe di inferiore rischio.

	garantiscono la totale efficacia oppure il controllo è stato implementato, ma è sporadicamente applicato.	
3- Adeguato	Le misure di sicurezza sono adeguate e sistematicamente applicate.	Tale livello comporta il passaggio a due classi inferiori di rischio.

In esito alla valutazione delle misure di sicurezza, queste risultano *parzialmente adeguate*. Infatti, come esplicitato al paragrafo che segue, *Definizione di un piano di azione*, sono stati riscontrati degli spunti di miglioramento nella gestione dei dati relativi alle segnalazioni *whistleblowing,* tra cui si ricorda possono esservi anche i cc.dd. dati relativi a condanne e reati, che possono porre a rischio i diritti e le libertà degli interessati.

Ne deriva, dunque, che il rischio residuo sia medio, in quanto dalla classe di rischio astratto elevato, considerando il livello delle misure di sicurezza parzialmente adeguato, il rischio residuo è di una classe inferiore.
Non è quindi necessario procedere con la consultazione preventiva all'Autorità Competente.

Definizione piano di azione:

- **Per una completa politica di no-log dei dati del segnalante e quindi per limitare ogni possibile tracciamento delle visite dei segnalanti o possibili segnalanti è necessario istruire i firewall del Titolare del trattamento inserendo delle regole di esclusione dei log per gli accessi alla Piattaforma e di ANAC canale esterno.**
- **Si suggerisce di erogare una formazione specifica anche in materia di privacy ai dipendenti del Titolare e al Gestore della segnalazione.**

COINVOLGIMENTO DELLE PARTI INTERESSATE

Oltre alla consultazione del Responsabile per la protezione dei dati (DPO), possono essere anche consultate le parti interessate (o il loro rappresentanti), se ritenuto opportuno. In tal modo, si garantisce una visione complessiva del processo e si conferisce maggior trasparenza alle modalità di svolgimento di tale attività.

- **Modalità di coinvolgimento del DPO: il DPO è stato coinvolto mediante invio in bozza della presente Relazione, sul quale lo stesso è stato chiamato ad esprimere parere, come previsto dal GDPR.**
- **Descrizione delle modalità attraverso le quali si sono consultate le parti interessate (e.g. questionari, incontri, sessioni o gruppi di lavoro): l'analisi del rischio e la successiva DPIA sono state condotte attraverso l'istituzione di un apposito gruppo di lavoro formato da consulenti esperti in materia di privacy e dal gruppo di lavoro "compliance".**
- **Della procedura di Gestione delle Segnalazioni deve essere data informativa alle rappresentanze sindacali.**

CONVALIDA FORMALE

Il Titolare del trattamento decide formalmente sull'accettabilità delle misure prescelte, dei rischi residui e del piano di azione, in modo ben motivato, anche a seguito delle consultazioni con DPO e interessati.

La valutazione d'impatto è:

- **Validata e Condizionata al miglioramento**

ORGANIZZAZIONE COINVOLTA E TEAM DI LAVORO

Descrizione dell'organizzazione nell'ambito della quale è stata svolta la valutazione d'impatto

- **Funzione: RPCT**
- **Periodo di esecuzione della valutazione: lug-2023 – dicembre 2023**

RIESAME E AGGIORNAMENTO
Indicare periodicità della revisione stabilita, nonché *owner* del processo: l'*owner* del processo è RPCT che è tenuto a rivedere la valutazione in caso di aggiornamento della normativa o dei processi interni, con il supporto del DPO.

Messina, 13 dicembre 2023

PER IL TITOLARE DEL TRATTAMENTO

Il Dirigente

f.to Dott. Arturo Vallone