DATA PROTECTION IMPACT ASSESSMENT

(*DPIA art. 35 REG UE 2016/679*)

SUL TRATTAMENTO DEI DATI PERSONALI INERENTI ALLA GESTIONE DELLE SEGNALAZIONI INTERNE DEL SISTEMA WHISTLEBLOWING

INFORMAZIONI ESSENZIALI

Data inizio analisi: 2 febbraio 2024
Data chiusura analisi: 11 marzo 2024
Data di confronto con il Titolare del trattamento: 8 marzo 2024
Versione: 00
Prossimo aggiornamento: entro il mese di marzo 2025

Titolare del trattamento: ORDINE PROVINCIALE DEI MEDICI E DEGLI ODONTOIATRI DI PERUGIA– Ente pubblico non economico di seguito (l'"Ente")

Responsabile del trattamento: Whistleblowing solution
Sub-responsabile del trattamento: Seeweb e Trasparency International Italia

DPO nominato: avv. Silvia Boschello

Consulente esterno scelto per la conduzione della DPIA: avv. Alexander Cassisa

SOMMARIO

1. PREMESSA

1.1 Introduzione

Nel mese di marzo 2023 è entrato in vigore il D. Lgs 10 marzo 2023 n. 24 (divenuto applicabile dal 15 luglio 2023) in materia di Whistleblowing in attuazione della Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 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.

L'obbligo di predisporre i canali di segnalazione interna agli enti e organizzazioni destinatari della normativa, grava, tra gli altri, sulle amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165 tra le quali rientra anche l'Ordine professionale dei Medici e degli Odontoiatri in qualità di ente di diritto pubblico.

La normativa, al fine di proteggere i dati delle persone che segnalano violazioni, dedica ampio spazio alla materia della protezione dei dati personali, in particolare prevedendo al comma sesto dell'art. 13 del succitato decreto che "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*."

La valutazione d'impatto sulla protezione dei dati (in inglese Data Protection Impact Assesment, "DPIA") è disciplinata all'art. 35 del Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (di seguito "GDPR"); si tratta di un processo inteso a descrivere uno specifico trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali, valutando detti rischi e determinando le misure organizzative e di sicurezza, per affrontarli. Secondo quanto previsto dall'art. 35, par. 1, GDPR, il Titolare del trattamento effettua una valutazione d'impatto sulla protezione dei dati quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".

Sempre in base alla normativa sul Whistleblowing ogni trattamento di dati personali, compresa la comunicazione tra le autorità competenti, previsto dal decreto n. 24, deve essere effettuato a norma del GDPR, del decreto legislativo 30 giugno 2003, n. 196 (norme relative al corretto trattamento dei dati personali delle persone fisiche da parte dei privati e degli enti pubblici) e del decreto legislativo 18 maggio 2018, n. 51 (norma relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché' alla libera circolazione di tali dati).
I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni devono effettuati dai titolari del trattamento, nel rispetto dei principi di cui agli articoli 5, 13 e 25 del GDPR.

I diritti di cui agli articoli da 15 a 22 del GDPR possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196: " 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 alla riservatezza della identità del segnalante".

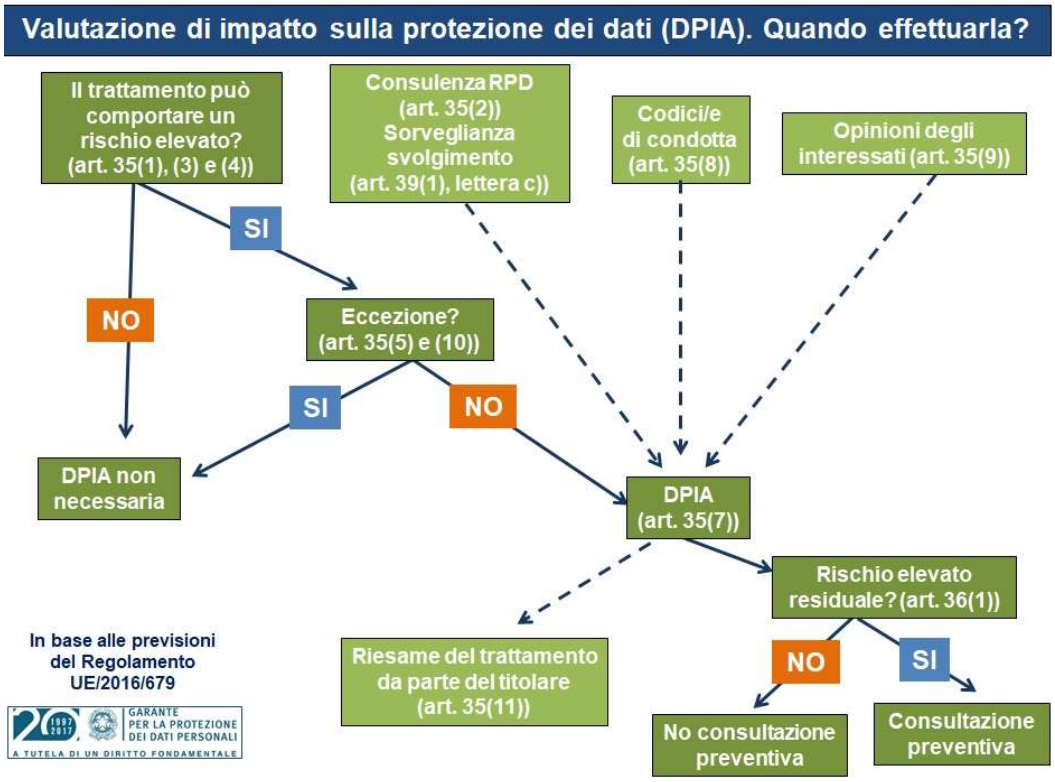
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

L'Ente una volta definito il proprio modello di ricevimento e gestione delle segnalazioni interne, deve individuare le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del Reg. (UE) 2016/679.

La responsabilità della valutazione dei rischi è in capo al Titolare del trattamento. Tuttavia, lo svolgimento della DPIA può essere affidato anche a un soggetto esterno all'organizzazione. Rimane compito del Titolare però la supervisione della sua redazione, anche in accordo e con la collaborazione del DPO nominato e per i trattamenti che lo richiedono anche con il parere e/o la collaborazione dell'amministratore di sistema.

1.2 Riferimenti normativi

- Artt. 35 e 36 del Reg. UE 2016/679 (anche "GDPR")
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679, adottate dal WP29 il 4 aprile 2017 e successivamente emendate il 4 ottobre 2017
- Provvedimento del Garante "Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018, che in data 19 novembre 2018 è stato pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269.
- D. Lgs 10 marzo 2023 n. 24 "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. (23G00032) (GU Serie Generale n.63 del 15-03-2023). Entrata in vigore del provvedimento: 30/03/2023.
- Linee guida ANAC - approvate con Delibera ANAC n°311 del 12 luglio 2023 - in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne.



2. DESCRIZIONE E ANALISI DEL CONTESTO

2.1 Il sistema di segnalazione del Whistleblowing e il relativo trattamento dei dati personali.

Il Whistleblowing è il sistema di segnalazione a tutela e protezione delle persone che denunciano violazioni di disposizioni normative nazionali o dell'Unione europea, che ledono l'interesse pubblico o l'integrità dell'amministrazione, di cui siano venute a conoscenza in un contesto lavorativo.

I canali di segnalazione si suddividono in:

- canale interno all'Ente (nell'ambito del contesto lavorativo);
- canale esterno (ANAC);
- divulgazione pubblica (tramite la stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
- denuncia all'Autorità giudiziaria o contabile.

L'Ente definisce una procedura che disciplina le modalità di segnalazioni interne (canali interni) e, in particolare:

- definisce l'ambito di applicazione del processo di segnalazione;
- identifica i soggetti che possono effettuare le segnalazioni e che sono tutelati secondo le disposizioni del d.lgs. 24/2023;

- circoscrive l'oggetto e i contenuti della segnalazione secondo le previsioni di cui al d.lgs. 24/2023;

- identifica e disciplina i canali interni attraverso cui effettuare la segnalazione interna all'Ente;

- identifica e prescrive i principi e le regole generali che governano il processo di segnalazione interno dell'Ente, nonché le conseguenze di eventuali abusi nell'utilizzo dei canali istituiti;

- definisce il processo di gestione della segnalazione nelle sue varie fasi, identificando ruoli, responsabilità, modalità operative e strumenti utilizzati.

L'Ordine professionale dei Medici e degli Odontoiatri di Perugia ha definito il proprio processo di gestione della segnalazione denominato "*PROCEDURA PER LA GESTIONE DELLE SEGNALAZIONI INTERNE DI VIOLAZIONI DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE DI CUI IL SEGNALANTE È VENUTO A CONOSCENZA NEL CONTESTO LAVORATIVO (WHISTLEBLOWING)* " documento approvato con Delibera del 12.02.20244, la quale è stata altresì sottoposta al vaglio del DPO (allegato 1).
La procedura è contenuta nel P.T.P.C.T., nella apposita sezione trasparenza del sito istituzionale dell'Ente, nel quale sono disciplinati i termini e le competenze specifiche per la gestione delle segnalazioni di illecito ricevute.
La Procedura è corredata da un "*MODELLO PER LA SEGNALAZIONE INTERNA DI VIOLAZIONI DI DISPOSIZIONI NORMATIVE NAZIONALI O DELL'UNIONE EUROPEA CHE LEDONO L'INTERESSE PUBBLICO O L'INTEGRITÀ DELL'AMMINISTRAZIONE DI CUI IL SEGNALANTE È VENUTO A CONOSCENZA NEL CONTESTO LAVORATIVO (WHISTLEBLOWING)*" e da due comunicazioni di avvio del procedimento e di esito dello stesso.
La procedura interna è stata redatta dall'Ente tenendo conto necessariamente delle dimensioni della propria organizzazione e della sua esposizione ai rischi.
La presente DPIA prende come riferimento la procedura dell'Ente quale base di partenza della valutazione dei rischi che avrà ad oggetto il trattamento dei dati personali inerenti alla gestione delle segnalazioni effettuate per il tramite dei canali interni.

2.2 Soggetti coinvolti nel trattamento

SEGNALANTE	È il destinatario della procedura che effettua la Segnalazione. Secondo il d.lgs. 24/2023 i segnalanti sono: a) i **dipendenti delle amministrazioni pubbliche** di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, ivi compresi i dipendenti di cui all'articolo 3 del medesimo decreto, nonché i dipendenti delle autorità amministrative indipendenti di garanzia, vigilanza o regolazione; b) i **dipendenti degli enti pubblici economici**, degli enti di diritto privato sottoposti a controllo pubblico ai sensi dell'articolo 2359 del Codice civile, delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio; c) **i lavoratori subordinati di soggetti del settore privato**, ivi compresi i lavoratori il cui rapporto di lavoro è disciplinato dal decreto legislativo 15 giugno 2015, n. 81, o dall'articolo 54-bis del decreto-legge 24 aprile 2017, n. 50, convertito, con modificazioni, dalla legge 21 giugno 2017, n. 96;

	d) i **lavoratori autonomi**, ivi compresi quelli indicati al capo I della legge 22 maggio 2017, n. 81, nonché i titolari di un rapporto di collaborazione di cui all'articolo 409 del Codice di procedura civile e all'articolo 2 del decreto legislativo n. 81 del 2015; e) i **lavoratori o i collaboratori**, che svolgono la propria attività lavorativa presso l'Ente; f) i **liberi professionisti e i consulenti** che prestano la propria attività presso l'Ente; g) i **volontari e i tirocinant**i, retribuiti e non retribuiti, che prestano la propria attività per l'Ente; h) **le persone con funzioni di amministrazione, direzione, controllo**, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.
SEGNALATO /PERSONA COINVOLTA	È il soggetto (persona fisica o giuridica) nei confronti del quale viene attribuita la violazione segnalata da parte del segnalante
FACILITATORE	È il soggetto operante all'interno del medesimo contesto lavorativo del segnalante, che assiste la persona segnalante nel processo di segnalazione
PERSONE DEL MEDESIMO CONTESTO LAVORATIVO	Sono le persone del medesimo contesto lavorativo della persona segnalante e che sono legate ad essa da uno stabile legame affettivo o di parentela entro il quarto grado.
COLLEGHI DI LAVORO	Colleghi di lavoro che lavorano nel medesimo contesto lavorativo del segnalante e che hanno con la persona che segnala un rapporto abituale e corrente.
ENTI DI PROPRIETA' PRIVATA	Ente di proprietà della persona segnalante (sia i casi in cui un soggetto è titolare di un ente in via esclusiva, sia in compartecipazione maggioritaria con terzi).
ENTI PER IL QUALE IL SEGNALANTE LAVORA	Enti per i quali il segnalante lavora (Ci si riferisce, a titolo esemplificativo, alla situazione in cui il dipendente di un'impresa che effettua un servizio di fornitura per un'amministrazione segnali o denunci una violazione avvenuta in quest'ultima)
ENTI CHE OPERANO NEL MEDESIMO CONTESTO LAVORATIVO	Enti che operano nel medesimo contesto lavorativo del segnalante anche se non di proprietà. Si tratta di enti, sia del settore pubblico che privato, che non hanno un vero e proprio legame diretto con il segnalante né sotto il profilo della proprietà né in quanto quest'ultimo vi presti lavoro o servizio.
R.P.C.T.	È il responsabile nominato ai sensi della L. 190/2012 ed è il destinatario delle segnalazioni della presente procedura.

ANAC	Autorità nazionale anticorruzione
ISTRUTTORE	Soggetto che fa parte della struttura di supporto del RPCT che è coinvolto nell'analisi della segnalazione e nella eventuale istruttoria. Ha accesso a tutte le informazioni inserite nelle segnalazioni se autorizzato dal RPCT ed è soggetto ai medesimi vincoli di riservatezza.

2.3 Dati personali trattati, interessati, processi e risorse di supporto

QUALI SONO I DATI TRATTATI	La Segnalazione dovrebbe contenere una chiara descrizione dei fatti oggetto di segnalazione, con indicazione della tipologia della violazione, delle circostanze di tempo e luogo in cui sono stati commessi/omessi i fatti, facendo emergere quanto più possibile: - la tipologia di violazione segnalata; -la lesione dell'interesse pubblico o dell'integrità; - le ragioni connesse al contesto lavorativo del segnalante. Infatti, le violazioni segnalate devono riguardare situazioni, fatti, circostanze, di cui il segnalante sia venuto a conoscenza in ragione del contesto lavorativo. Dati personali che potrebbero essere trattati sono dati: - identificativi e di contatto dei soggetti coinvolti nella segnalazione; - relativi al contenuto della segnalazione con utilizzo possibile anche di dati appartenenti alle categorie dei dati particolari e di dati relativi a condanne penali e reati; - eventualmente contenuti in atti e documenti conseguenti alla segnalazione stessa.
INTERESSATI E INFORMATIVE	Le categorie di soggetti interessati al presente trattamento, sono: ● segnalante; ● segnalato; ● facilitatori; ● terzi soggetti coinvolti nella segnalazione. Gli interessati sono informati sul trattamento dei propri dati personali per mezzo della informativa art. 13 GDPR relativa a "INFORMAZIONI AI SENSI DELL'ART. 13 DEL REGOLAMENTO (UE) 2016/679 SUL TRATTAMENTO DEI DATI PERSONALI DEI SOGGETTI CHE SEGNALAZIONI ILLECITI-WHISTLEBLOWING D. Lgs 10 marzo 2023 n. 24 in materia di Whistleblowing che attua la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 23 ottobre 2019". Il link all'informativa è inserito nella modulistica e pubblicato, altresì, nel sito istituzionale dell'Ente (allegato 2).
CICLO DI VITA DEL TRATTAMENTO DEI DATI (DESCRIZIONE FUNZIONALE)	La ricezione della segnalazione avviene tramite canali interni, scritti o orali. Le segnalazioni devono essere adeguatamente documentate e conservate in forma recuperabile e verificabile, conformemente alle prescrizioni in materia di riservatezza e protezione dei dati. L'iter di accertamento della segnalazione da parte del RPCT è il seguente: -entro 7 gg dalla segnalazione l'RPCT comunica al segnalante la ricezione dell'istanza;

	-entro 15 gg dalla segnalazione l'RPCT decide sull'ammissibilità della segnalazione; -entro 90 gg dalla segnalazione l'RPCT comunica al segnalante l'esito o lo stato di avanzamento del procedimento. Laddove si renda necessario, l'organo di indirizzo politico può autorizzare il RPCT ad estendere i predetti termini a fronte di richiesta motivata da parte del RPCT. La segnalazione se del caso potrà essere trasmessa alle Autorità giudiziarie competenti per i profili di competenza.
I CANALI DI SEGNALAZIONE	**Segnalazioni interne:** 1. **canale scritto tradizionale:** la segnalazione viene effettuata per il tramite del servizio postale l'Ente dovrebbe ricevere la segnalazione contenuta in una busta chiusa indirizzata al RPCT (con dicitura esterna Riservata Personale Whistleblowing). Il segnalante può scaricare la modulistica reperibile sul sito web istituzionale nella Sezione "Amministrazione Trasparente" sottosezione "Altri contenuti - Prevenzione della Corruzione". *** 2. **canale informatico crittografato.** L'Ente di avvale per le segnalazioni per via elettronica di una piattaforma, denominata GlobaLeaks, che è un software gratuito basato su una infrastruttura Iaas e Saas, Open Source, realizzata da Whistleblowing Solutions Impresa Sociale, che è stata appositamente nominata ex art. 28 GDPR, responsabile esterna del trattamento, fornitore ritenuto dal Titolare fornitore affidabile sulla base di quanto dichiarato nella documentazione contrattuale e tecnica visto che lo stesso è dotato di standard e certificazioni ISO sulla sicurezza delle informazioni. Il Segnalante entrando nel sito istituzionale dell'Ente nella sezione dedicata alle segnalazioni whistleblowing può accedere alla piattaforma di segnalazione tramite l'indirizzo web www. https://www.ordinemediciperugia.it/ La segnalazione viene redatta dal segnalante attraverso la compilazione di un apposito questionario guidato, che è stato studiato e condiviso anche a livello internazionale all'interno del progetto di Transparency International Italia che è un'organizzazione no profit, parte del network globale di Transparency International che è una ONG che si occupa di anticorruzione a livello mondiale. La segnalazione viene ricevuta dal RPCT che riceverà una e-mail sulla casella di posta elettronica istituzionale dedicata alla ricezione delle segnalazioni, che notifica la presenza di una nuova segnalazione nel portale del Whistleblowing, a cui accede dal link presente nel corpo dell'e-mail. Il RPCT è l'unico soggetto ad avere le password di accesso alla casella di posta elettronica istituzionale dedicata alla ricezione delle segnalazioni e al portale online. Il portale richiede username e password in possesso del solo RPCT per accedere alla lista delle Segnalazioni. La password dovrà essere cambiata, a cura del RPCT ogni 90 giorni. Il RPCT per visualizzare la nuova segnalazione dovrà selezionarla dalla lista. Il portale consente una registrazione cronologica delle segnalazioni con registrazione della data e dell'ora di ricezione delle segnalazioni.

	Il custode dell'identità del segnalante è lo stesso RPCT. La segnalazione è accessibile esclusivamente dal RPCT in quale potrà autorizzare un soggetto istruttore a coadiuvarlo nella gestione dell'istanza (v. allegato 3). Il soggetto istruttore è soggetto ai medesimi obblighi di riservatezza del RPCT la cui violazione è punita a livello disciplinare. In ogni caso, il RPCT avrà l'onere di mantenere riservati i dati identificativi del segnalante e il contenuto della segnalazione. Il segnalante è tenuto a compilare, in modo chiaro, preciso e circostanziato le "sezioni" del questionario fornendo le informazioni richieste come obbligatorie e il maggior numero di quelle facoltative. - nel momento dell'invio della segnalazione, il segnalante riceve un codice identificativo univoco (key code) che gli/le permette di accedere alla propria segnalazione/comunicazione. Ciò consente al segnalante di "dialogare", di allegare documenti e di esser informato sullo stato di lavorazione della segnalazione inviata. - Il key code non può essere replicato. È onere del segnalante averne adeguata cura. In caso di smarrimento del key code, il whistleblower non può più collegarsi alla propria segnalazione per fornire specificazioni o ulteriore documentazione. - Il sistema garantisce l'informativa automatica al segnalante circa la presa in carico della segnalazione, la possibilità di essere ricontattato per acquisire elementi utili alla fase istruttoria, la possibilità di inviare ulteriori informazioni di cui verrà eventualmente a conoscenza ai fini dell'integrazione dei fatti oggetto di segnalazione. - L'applicativo è inoltre utilizzato per dare comunicazione al segnalante della chiusura dell'istruttoria. Le informazioni raccolte sono custodite in formato elettronico sulla piattaforma, dotata di profili definiti di accesso, autenticazione obbligatoria e tracciamento automatico delle operazioni svolte. - L'applicativo tutela l'identità del segnalante, il quale potrà scrivere ed inviare la segnalazione anche in forma anonima questo perché la piattaforma permette il dialogo, anche in forma anonima, tra il segnalante e il responsabile per il whistleblowing per richieste di chiarimenti o approfondimenti, senza quindi la necessità di fornire contatti personali. Il segnalante potrà effettuare la segnalazione da qualsiasi dispositivo digitale (pc, tablet, smartphone), sia dall'interno dell'Ente che dal suo esterno. La tutela della riservatezza è garantita in ogni circostanza. Al segnalante è consentito di verificare, in qualsiasi momento tramite l'applicazione, lo stato di avanzamento dell'istruttoria. 3. **canale orale:** Le segnalazioni **in forma orale** sono effettuate anche attraverso un incontro diretto con RPCT e/o uno con il soggetto istruttore appositamente nominato, su richiesta del segnalante. Durante l'incontro sarà verbalizzata la segnalazione e consegnata l'informativa art. 13 GDPR (v. allegato 2). **** Il RPCT una volta ricevuta la segnalazione, ottenuta in qualunque forma di canale interno, la registrerà sul registro delle segnalazioni whistleblowing fornendo una numerazione progressiva per ciascuna segnalazione.

	Il contenuto della segnalazione e il nominativo del soggetto segnalante saranno inseriti in una busta chiusa al cui esterno verrà indicato solo il numero progressivo di segnalazione. Il registro delle segnalazioni, la segnalazione, il nominativo del segnalante nonché tutti gli accertamenti istruttori del caso saranno conservati presso la sede dell'Ente in armadio dedicato provvisto di chiusura, le cui chiavi sono nella esclusiva disponibilità del RPCT. Il RPCT potrà autorizzare un soggetto istruttore, debitamente formato sulla disciplina e la procedura, a coadiuvarlo nella gestione dell'istanza. L'istruttore sarà nominato autorizzato al trattamento ex art. 29 GDPR e debitamente formato sulla disciplina e sulle procedure interne all'Ente (allegato 3). Il soggetto istruttore è soggetto ai medesimi obblighi di riservatezza del RPCT la cui violazione è punita a livello disciplinare. In ogni caso, il RPCT avrà l'onere di mantenere riservati i dati identificativi del segnalante e il contenuto della segnalazione.

2.4 Principi fondamentali

RISERVATEZZA	L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate **senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni.** Più precisamente nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 c.p.p. Nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria. Nell'ambito del procedimento disciplinare, l'identità della persona segnalante non può essere rivelata, ove 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 della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità. I corollari della tutela della identità del segnalante: a) preferenza per la gestione informatizzata delle segnalazioni, con il ricorso a strumenti di crittografia; b) sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso privacy, amministrativo e generalizzato c) oscuramento dei dati quando possibile. La riservatezza, oltre che all'identità del segnalante, viene garantita anche a qualsiasi altra informazione o elemento della segnalazione dal cui disvelamento si possa dedurre direttamente o indirettamente l'identità del segnalante. La riservatezza viene garantita anche nel caso di segnalazioni - interne o esterne - effettuate in forma orale su richiesta della persona segnalante, mediante un incontro diretto con chi tratta la segnalazione. Si tutela la riservatezza del segnalante anche quando la segnalazione perviene a personale diverso da quello

	autorizzato e competente a gestire le segnalazioni, al quale, comunque, le stesse vanno trasmesse senza ritardo In due casi espressamente previsti dal decreto, per rivelare l'identità del segnalante, oltre al consenso espresso dello stesso, si richiede anche una comunicazione scritta delle ragioni di tale rivelazione o nel procedimento disciplinare laddove il disvelamento dell'identità del segnalante sia indispensabile per la difesa del soggetto a cui viene contestato l'addebito disciplinare; nei procedimenti instaurati in seguito a segnalazioni interne o esterne laddove tale rivelazione sia indispensabile anche ai fini della difesa della persona coinvolta. Tutela della riservatezza deve riguardare anche il facilitatore che assiste il segnalante Tutela della riservatezza deve coinvolgere anche le persone differenti dal segnalato ma menzionate nella segnalazione, tramite il ricorso a strumenti di crittografia ove si utilizzino strumenti informatici. La persona segnalata può essere sentita o viene sentita, dietro sua richiesta, anche mediante procedimento cartolare attraverso l'acquisizione di osservazioni scritte e documenti. Tale soggetto non ha il diritto di essere sempre informato della segnalazione che lo riguarda ma solo nell'ambito del procedimento eventualmente avviato nei suoi confronti a seguito della conclusione della gestione della segnalazione e nel caso in cui tale procedimento sia fondato in tutto o in parte sulla segnalazione. L'Ente dovrebbe essere in grado di accettare e dare seguito alle segnalazioni anonime e tutelare i whistleblower anonimi. L'Ente dovrebbe vietare qualsiasi forma di ritorsione - atto o omissione minacciata, raccomandata o effettiva, diretta o indiretta, che causa o possa causare danno - connessa alla segnalazione di irregolarità, nonché qualsiasi interferenza con la segnalazione di illecito. I segnalanti confidenziali sono coloro che scelgono sin da subito di far sapere chi sono. Rivelano ad esempio il loro nome, cognome o un loro contatto quale il numero telefonico o l'indirizzo e-mail, che talvolta consentono una comunicazione più diretta e veloce. La segnalazione resta tuttavia riservata: l'identità del segnalante non viene rivelata a meno che non si abbia il suo esplicito consenso. I segnalanti anonimi, invece, solo coloro che preferiscono non fornire alcuna informazione, almeno in prima battuta. La piattaforma consente ai segnalanti di contattare l'Ente anche in modo anonimo, mantenendo aperta la possibilità di dialogo, così da approfondire e chiarire le informazioni inviate. Ciò che realmente interessa, a prescindere dalla conoscenza o meno dell'identità del segnalante, è il rimedio alle condotte illecite segnalate. Il segnalante è pertanto libero di scegliere se rivelare il suo nome, non farlo oppure farlo durante il dialogo. **Si ribadisce che occorre avere massima cautela in tema di riservatezza, in modo particolare quando l'istruttoria richiede il coinvolgimento di altri soggetti.** In merito a quanto sopra previsto rispetto al ciclo di vita della segnalazione (v. sopra pag. 7 art.2.3) laddove si renda necessario estendere la segnalazione all'organo di indirizzo politico (ad esempio se deve autorizzare il RPCT ad estendere i termini a fronte di richiesta motivata da parte dello stesso RPCT) si consiglia caldamente all'Ente ed in particolare al RPCT **l'oscuramento dei dati.** Tale obbligo di riservatezza si estende anche al contenuto della segnalazione, allegati compresi, nel

	caso in cui da questi dati si possa risalire all'identità del segnalante anche indirettamente. Ciò, naturalmente, si traduce nella sottrazione della segnalazione e della documentazione ad essa allegata al diritto di accesso agli atti amministrativi previsto dagli artt. 22 e ss. della legge 241/1990. Il RPCT che riceve la segnalazione può, naturalmente, ove il caso lo richieda, inoltrare la segnalazione alle Autorità giudiziarie competenti, comunicando che si tratta di una segnalazione whistleblowing e che, perciò, la riservatezza del segnalante è tutelata. Nel caso in cui, però, l'Autorità giudiziaria o contabile chieda di fornire i dati del segnalante, il RPCT è tenuto a fornirli, dopo averne dato notifica al segnalante.
TRASPARENZA	L'Ente si impegna a mettere a disposizione 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. Le suddette informazioni sono esposte e rese facilmente visibili nei luoghi di lavoro, nonché accessibili alle persone che, pur non frequentando i luoghi di lavoro intrattengono un rapporto giuridico con l'Ente, il quale pubblica le suddette informazioni in una sezione dedicata del sito web istituzionale. Gli interessati sono informati attraverso l'informativa sul trattamento dei dati personali relativa a "INFORMAZIONI AI SENSI DELL'ART. 13 DEL REGOLAMENTO (UE) 2016/679 SUL TRATTAMENTO DEI DATI PERSONALI DEI SOGGETTI CHE SEGNALAZIONI ILLECITI- WHISTLEBLOWING D. Lgs 10 marzo 2023 n. 24 in materia di Whistleblowing che attua la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 23 ottobre 2019" (v. allegato 3)
ADEGUATEZZA, PERTINENZA E LIMITAZIONE A QUANTO È NECESSARIO IN RELAZIONE ALLA FINALITA'	I dati trattati sono: - adeguati, perché non eccedenti rispetto alle finalità di gestire e dare seguito alle segnalazioni; - pertinenti, perché strettamente connessi ai processi interni gestiti dall'Ente mediante policy e formazione dedicata al RPCT e al personale dell'Ente; - limitati, perché l'Ente deve limitare la raccolta e la gestione a ciò che è strettamente necessario avendo cura di comprovare che le informazioni siano sufficienti, pertinenti e non eccessive, deve inoltre limitate la trasmissione di documenti elettronici contenenti dati personali allo stretto necessario
ESATTEZZA AGGIORNAMENTO	L'RPCT deve assicurarsi, nei limiti delle proprie competenze e possibilità, che i dati siano esatti e aggiornati. L'aggiornamento dei dati all'interno della piattaforma è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali relativi alle comunicazioni e a ogni tipo di aggiornamento.

PERIODO DI CONSERVAZIONE DEI DATI	L'Ente dovrà conservare ogni segnalazione ricevuta, conformemente ai requisiti di riservatezza. Le segnalazioni dovrebbero essere conservate per un periodo di tempo non superiore a quello necessario e in modo proporzionato e conforme agli obblighi di legge che stabiliscono il termine **di non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura** di segnalazione.
DEFINIZIONE DEGLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO E FORMALIZZAZIONE DEI CONTRATTI	I responsabili del trattamento sono nominati con apposito accordo *ex* art. 28, Regolamento (UE) 2016/679. Gli stessi assicurano garanzie sufficienti per porre in atto misure tecniche e organizzative adeguate, in modo tale che il trattamento dei dati soddisfi i requisiti richiesti dal Regolamento e dalla normativa nazionale, al fine di garantire la massima tutela dei diritti degli interessati. In caso di intervenuta violazione di dati personali, saranno attuate le *policy* per la gestione dei *data breach* già in uso presso i soggetti coinvolti.
TRASFERIMENTO DATI	Non è previsto il trasferimento di dati all'estero.

2.5 Finalità del trattamento

La finalità del trattamento è:

- specifica, in quanto consistente nella raccolta e gestione dei dati personali relativi ad una segnalazione whistleblowing di presunte condotte illecite effettuate dai dipendenti e dai collaboratori dell'Ente sia il rapporto di lavoro intercorrente (dipendente, autonomo, di diritto privato, di consulenza, di collaborazione, di somministrazione) e dai lavoratori e collaboratori delle imprese fornitrici di beni o servizi e che realizzano opere in favore dell'Ente stesso;

- esplicita, in quanto rientrante tra i motivi di interesse pubblico rilevante perseguiti a nazionale, europeo a protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali.

- lecita, in quanto basata su un obbligo di legge, cioè la normativa vigente sul Whistleblowing: D. Lgs 10 marzo 2023 n. 24 in materia di Whistleblowing che attua la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 23 ottobre 2019.

In particolare, i dati personali verranno trattati per svolgere le necessarie attività istruttorie volte a verificare la fondatezza di quanto segnalato, nonché se del caso, adottare misure correttive ed informare dell'esito dell'istruttoria le autorità competenti (autorità giudiziaria e soggetti titolari dell'azione disciplinare). I dati personali sono trattati dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) nell'esecuzione di compiti di interesse pubblico nonché in base ad obblighi di legge a cui è soggetto il titolare del trattamento, con particolare riferimento al compito di gestire le segnalazioni di condotte illecite presentate dai dipendenti e collaboratori dell'Ente.

2.6 Base giuridica del trattamento

L'Ente in qualità di Titolare del trattamento è tenuto a fornire al segnalante le informazioni riguardanti il trattamento dei dati personali che lo riguardano in relazione alla attività di segnalazione di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica di cui l'interessato sia venuto a conoscenza nel contesto lavorativo pubblico o privato. La base giuridica del trattamento è la normativa vigente sul Whistleblowing: D. Lgs 10 marzo 2023 n. 24 in materia di Whistleblowing che attua la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, 23 ottobre 2019.

In particolare, ogni trattamento di dati personali, compresa la comunicazione tra le autorità competenti, previsto dal decreto n. 24/2023, deve essere effettuato a norma del Reg. UE 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51. I trattamenti di dati personali relativi al ricevimento e alla gestione delle Segnalazioni sono effettuati dai titolari del trattamento, nel rispetto dei principi di cui agli articoli 5, 13 e 25 del Reg. (UE).

2.7 Esercizio dei diritti da parte degli interessati

I diritti riconosciuti agli interessati dal Regolamento (UE) 2016/679, in quanto compatibili, possono essere esercitati secondo le seguenti modalità:

I diritti di cui agli articoli da 15 a 22 del Reg. UE possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196: " 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 alla riservatezza della identità del segnalante".

L'interessato potrà esercitare i seguenti diritti, quali:

- l'accesso ai Dati personali;
- la rettifica dei dati in possesso;
- la cancellazione di qualsiasi dato per il quale l'ente non abbia più alcun presupposto giuridico per il trattamento;
- la limitazione del trattamento;
- l'opposizione al trattamento;
- la copia dei Dati Personali forniti (c.d. portabilità);
- il reclamo al Garante per la protezione dei dati personali, nel caso l'interessato ritenga che il trattamento dei dati personali avvenga in violazione di quanto previsto dal GDPR, utilizzando i riferimenti disponibili nel sito internet dell'autorità.

Nel caso in cui l'Interessato esercitasse uno qualsiasi dei già menzionati diritti, sarà onere dell'Ente verificare che l'interessato sia legittimato ad esercitarlo soprattutto alla luce possono dei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196, lo stesso ente darà riscontro, di regola, entro un mese.

L'apposita istanza al RPTC è presentata contattando il medesimo presso l'Ordine ovvero contattando il responsabile della protezione dei dati personali (DPO) nominato dall'Ente.

3. VALUTAZIONE DEI RISCHI

3.1 L'analisi

L'analisi dei rischi è finalizzata ad individuare il livello di esposizione al rischio dei dati personali trattati. I risultati dell'analisi consentiranno di individuare gli ambiti su cui focalizzare gli interventi, ottimizzando l'impiego delle risorse a disposizione dell'Ente. La valutazione dei rischi è un'attività complessa e delicata che non si può sostanziare in una mera rappresentazione sintetica di dati e numeri. Le scelte e le decisioni che ne derivano implicano un'assunzione di responsabilità che deve essere necessariamente documentata (accountability) attraverso strumenti formali che permettano di motivare i passaggi metodologici seguiti nonché rendere palesi i criteri sulla base dei quali sono stabiliti pesi e misure per ogni fattore preso in considerazione.

3.2 Il monitoraggio

L'Ente è tenuto a svolgere un monitoraggio del sistema whistleblowing, attraverso obiettivi di controllo, per valutare:

- ✓ l'effettivo stato di implementazione delle misure di sicurezza,
- ✓ l'efficacia delle misure implementate,
- ✓ l'effettiva e corretta applicazione del framework,
- ✓ la conformità ai requisiti del Regolamento al fine di valutarne l'efficacia nel tempo.

3.3 Stima dei rischi connessi al trattamento

La mappatura dei rischi prevede l'indicazione di queste voci:

A. **Scenario,** cioè il contesto in cui sono elencati i rischi individuati

B. **Nome della minaccia**, cioè, qualsiasi circostanza o evento che potenzialmente può determinare un impatto negativo (un male o un danno) sui dati dell'interessato. La scelta del tipo di minaccia da prendere in considerazione al loro potenziale di rischio dovrà ricadere, ovviamente, su quelle che si presentano caratterizzanti per l'organizzazione in relazione ai tipi di trattamento svolto e al contesto in cui detti trattamenti si svolgono.

Area d'impatto (C; D; E):

C. Riservatezza: protezione del dato da accessi non autorizzati. Riservatezza, cioè la proprietà di un'informazione volta a garantire che la stessa sia accessibile esclusivamente ai soggetti e/o ai processi legittimamente autorizzati. Tale requisito

implica che i dati siano gestiti in sicurezza in modo tale da mitigare il rischio di accesso ai dati o di loro utilizzo non autorizzato;

D. Disponibilità, cioè la proprietà che un'informazione sia accessibile ed utilizzabile a fronte di una richiesta autorizzata. Tale requisito implica che i dati debbano essere salvaguardati in modo che ne sia garantito l'accesso, l'usabilità e la confidenzialità. Da un punto di vista di gestione dei rischi, significa ridurre a livelli accettabili i rischi connessi all'accesso alle informazioni (intrusioni, furto di dati, ecc.) garantendone la sicurezza;

E. Integrità, cioè la proprietà di un'informazione volta a garantire l'inalterabilità e/o la non modificabilità della stessa da parte di soggetti non legittimamente autorizzati. Tale requisito implica che i dati non vengano alterati, ossia non subiscano modifiche o cancellazioni a seguito di eventi esterni e/o di azioni deliberate e non (es. malfunzionamenti o danni degli asset che contengono i dati stessi).

Valutazione del rischio (F; G; H)

Il rischio è, la **probabilità** (F) che possa accadere qualcosa di negativo. Per far sì che si presenti l'eventualità di un rischio (H) è necessario avere sia un fattore di minaccia che un fattore di impatto (G). Il rischio consiste nella potenziale perdita, danno o distruzione di un'attività a seguito di una minaccia che sfrutta una vulnerabilità del sistema, processo o dell'organizzazione.

Quello che comunque da tenere sempre presente è che il livello della minaccia è calcolato sul trattamento, il livello di impatto è invece calcolato sugli interessati.

Il dato di partenza è la minaccia (correttamente individuata) a cui si deve associare l'indice di probabile accadimento. Su tale tipo di valutazione assumono rilevanza le misure di sicurezza che definiscono il livello di vulnerabilità di un dato trattamento. In sostanza l'assenza o la carenza di una misura di sicurezza non inciderà, quindi, sull'impatto ma sul livello di probabilità di accadimento della minaccia;

Il processo di valutazione consiste in una stima (in astratto) del danno/conseguenze che deriverebbero all'interessato qualora per un certo tipo di trattamento si verificasse una perdita di riservatezza, integrità o disponibilità del dato.

F. Probabilità: possibilità che accada un determinato evento capace di causare un danno agli interessati.

G. Impatto: gravità del danno generato dall'evento al momento della sua realizzazione o nel periodo successivo.

H. Rischio: eventualità che si verifichi un danno (rischio = probabilità x impatto).

Probabilità		
Valore	**Livello**	**Descrizione Qualitativa**

Improbabile	1	Eventi molto rari, desterebbero grande sorpresa
Poco probabile	2	Eventi occasionali e inattesi, desterebbero sorpresa
Probabile	3	Eventi possibili già occorsi in passato
Altamente probabile	4	Eventi già verificatisi di recente

Impatto		
Valore	**Livello**	**Descrizione Qualitativa**
Lieve	1	Il danno comporta effetti limitati ed è immediatamente risolvibile.
Moderato	2	Il danno comporta alcuni inconvenienti, che saranno risolvibili nonostante alcune difficoltà.
Grave	3	Il danno comporta conseguenze significative, che saranno risolvibili seppur con diverse difficoltà.
Molto grave	4	Il danno comporta conseguenze significativamente, irreversibili o risolvibili con estrema difficoltà.

Gestione del rischio			
Min	Max	Range	**Descrizione**
1	1	Trascurabile	Il rischio è di scarsa o nessuna rilevanza.
2	2	Lieve	Non sono necessarie ulteriori misure di sicurezza.
3	4	Modesto	È opportuno monitorare periodicamente le misure di sicurezza attuate e, se del caso, revisionarle, collaudarle e/o aggiornarle.
6	9	Accettabile	È appropriato pianificare nuove misure di sicurezza, revisionare/collaudare quelle già attuate nonché valutare l'opportunità di loro implementazione.
12	15	Alto	È necessario procedere a ulteriori analisi per individuare e pianificare ulteriori misure sicurezza, valutando l'opportunità di sospendere il trattamento.
16	16	Molto alto	È prioritario procedere a nuove analisi per individuare e pianificare ulteriori misure sicurezza prima di iniziare o proseguire il trattamento.

SCALA DI RISCHIO		**Probabilità**			
		1	**2**	**3**	**4**
Impatto	**4**	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4

Scala di Rischio del Trattamento: il rischio può essere qualitativamente espresso usando la scala sopra indicata.

Normalmente le organizzazioni preferiscono, come scelta strategica, quello che viene definito rischio accettabile. Ciò consente di sviluppare un piano di interventi, dando la priorità a quelli relativi ad eventi che presentino un livello di rischio stimato R > RA. È in questa fase che si decide se i livelli di rischio residuo risultano accettabili o richiedono un intervento.

Le possibili modalità di gestione dei Rischi sono tradizionalmente quattro:

- ACCETTARE: decidere di accettare il rischio, a fronte di una valutazione costi/benefici;

- RIDURRE: mitigare il rischio, ovvero ridurre il rischio ad un livello accettabile per il business, attraverso l'adozione di contromisure sostenibili;

- TRASFERIRE: trasferire il rischio ad altre parti (ad es. fornitori, outsourcer, società di assicurazione, ecc.);

- RIMUOVERE: evitare il rischio, rinunciando, ad esempio, ad effettuare il trattamento in esame. Solo qualora il rischio residuo sia ritenuto elevato, il Titolare del trattamento, prima di procedere al trattamento, consulterà l'autorità di controllo (la c.d. Consultazione preventiva, art. 36 GDPR).

Segue l'analisi dettagliata dei rischi del sistema Whistleblowing rappresentata in un documento Excel (allegato 4).

3.4 Considerazioni conclusive dell'analisi dei rischi

Alla luce di quanto sopra, tenuto conto degli impatti e quindi dei rischi potenziali, delle misure pianificate e implementate, i rischi vengono stimati come da tabella allegata sub 4. **Dai risultati dell'analisi i rischi rimangono all'interno del grado di accettabilità (colore giallo).**

Non sono rilevati rischi alti o altissimi per cui non è necessario procedere ad ulteriori analisi per individuare e pianificare ulteriori misure sicurezza, valutando l'opportunità di sospendere il trattamento. Né è necessario evitare il rischio, rinunciando, ad esempio, ad effettuare il trattamento in esame. Il Titolare del trattamento, quindi, prima di procedere al trattamento, non consulterà l'autorità di controllo (la c.d. Consultazione preventiva, art. 36 GDPR).

4. PIANO DI AZIONE-MISURE DI SICUREZZA

4.1 Il piano di azione

Costituisce un sostegno all'accountability, consente di definire un piano condiviso delle misure da adottare, delle responsabilità di esecuzione e di verifica, di assunzione da parte del Titolare, della consapevolezza del Rischio residuo. Si tratta di rilevare le misure idonee per ridurre probabilità e impatto. I controlli che il Titolare deve valutare per mitigare i rischi sul trattamento possono riguardare le misure descritte di seguito.

- Misure e controlli di tipo organizzativo: organizzazione e governance; specifici ruoli e responsabilità all'interno dell'organizzazione; controlli interni di supervisione; definizione dei ruoli per la gestione della procedura;
- Processi: procedure e policy interne, modelli di gestione dei rischi, gestione degli incidenti, delle modifiche e delle notifiche alle Autorità, contratti per proteggere le

informazioni trattate in ambiti esternalizzati, accordi che rendano evidente quali informazioni debbano essere condivise, come e con chi;

- Formazione e consapevolezza: formazione adeguata del personale e dei consiglieri dell'Ordine e consapevolezza dei potenziali rischi, selezione degli incaricati in base a qualifiche e competenze dimostrabili, guide operative per il personale su come adottare la nuova procedura e su come condividere i dati quando necessario,
- Materiale informativo per gli utenti, misure che consentano agli interessati di accedere alle proprie informazioni e al tempo stesso che rendano gli interessati consapevoli di come sono protette le proprie informazioni, di prevedere canali con cui gli utenti possano contattare l'organizzazione in caso di necessità di assistenza e con cui le organizzazioni possano rispondere alle richieste di accesso da parte degli interessati.

Molte di queste azioni sono descritte all'interno della valutazione dei rischi nell'allegato sub 4.

4.2 Misure di sicurezza da adottare

4.2.1 Canale TRADIZIONALE

Si consiglia al fine di maggiore garanzia di riservatezza nell'applicazione della procedura di migliorare le "istruzioni" a favore dell'utente/segnalante all'interno del sito web istituzionale; a titolo esemplificativo deve essere indicato al segnalante che la segnalazione deve essere inserita in una busta chiusa che rechi all'esterno la dicitura "riservata/personale", indirizzata al Responsabile della Prevenzione della Corruzione e della Trasparenza dell'Ente. E inoltre, altamente raccomandato che la segnalazione venga "guidata" attraverso un apposito modulo che deve essere allegato alla procedura e pubblicato nel sito web. Inoltre, la protocollazione della segnalazione pervenuta tramite posta cartacea dovrebbe avvenire tramite funzioni del sistema di gestione documentale che dovrebbero garantire la visibilità al solo al RPCT o ai soggetti istruttori, espressamente autorizzati i quali sono tenuti ad osservare gli obblighi di riservatezza. La violazione di tali obblighi comporta la violazione dei doveri d'ufficio con la conseguente responsabilità disciplinare ed irrogazione delle relative sanzioni.

4.2.2 Canale INFORMATICO

Questo canale rispetto al canale scritto tradizionale è da preferire ed incentivare, perché più sicuro in punto riservatezza e protezione dei dati personali.

Nello specifico, l'Ente si avvale dell'apposita piattaforma per l'acquisizione e la gestione delle segnalazioni messa a disposizione da Transparency International Italia e da Whistleblowing Solutions Impresa, nell'ambito del progetto WhistleblowingPA. La piattaforma è conforme alla normativa vigente e garantisce - attraverso il ricorso a strumenti di crittografia - la riservatezza dell'identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione.

Sono stati definiti dall'Ente gli accordi contrattuali con le società:

● Whistleblowing Solutions in qualità di Responsabile del trattamento appositamente nominato responsabile esterno ex art. 28 GDPR dall'Ente

● Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions

● Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions

L'applicativo GlobaLeaks dichiara di applicare le seguenti misure di sicurezza:

- CRITTOGRAFIA mediante uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington reperibile al link: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html;

- CONTROLLO ACCESSI LOGICI l'accesso è consentito ad utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema vieta l'uso di PW già utilizzate e implementa policy PW sicura nonché un protocollo di autenticazione a due fattori TOTP secondo gli standards RFC 6238.

- TRACCIABILITA' per il tramite di un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema di compatibilità con la massima confidenzialità richiesta dal processo whistleblowing. I log delle attività dei segnalante sono prive di informazioni identificative dei segnalanti quali indirizzi IP e User Agent. Mentre i log amministratori di sistema sono registrati tramite moduli syslog e registri remoti centralizzati.

- ARCHIVIAZIONE l'applicativo garantisce elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo stesso delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

- GESTIONE VULNERABILITA' TECNICHE l'applicativo e tutta la fornitura Saas sono soggetti a periodici audit di sicurezza (date anche le certificazioni ISO dichiarate) su base annuale che vengono pubblicati: https://docs.globaleaks.org/en/main/security/PenetrationTests.html .

- BACK UP tutti i sistemi dell'applicativo sono soggetti a back remoto giornaliero di date retention di 7 gg necessari per finalità di distaster recovery

- SICUREZZA DEI CANALI INFORMATICI tutte le connessioni sono protette tramite protocollo TLS1.2+ mentre le connessioni amministrative privilegiate dono mediate tramite accesso VPN con protocollo SSH.

- SICUREZZA DELL'HARDWARE mediante videosorveglianza e sistema di allarme e barriere fisiche presidiate e certificati ISO 27001.

- GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI mediante procedura data breach.

- USO DI METODOLOGIE standard conformi con la normativa vigente in ambito nazionale e internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing. A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

    - THREAT MODEL

    - APPLICATION SECURITY.

In data 25 ottobre 2023 il fornitore ha comunicato all'Ente che è stata rilasciata, l'ultima versione del software GlobaLeaks (versione 4.13.15) che prevede due importanti aggiornamenti.

- Il primo aggiornamento intende migliorare la gestione della documentazione relativa alla segnalazione direttamente sulla piattaforma, garantendo così tutti gli standard di sicurezza e riservatezza che caratterizzano il software. Il soggetto ricevente potrà infatti caricare, nella sezione dedicata agli allegati e commenti di ciascuna segnalazione, note o documenti necessari alla gestione della stessa. Sono previsti diversi livelli di visibilità della documentazione, a seconda delle necessità. I file potranno infatti essere visibili sia ai soggetti riceventi che al segnalante, oppure potranno essere visibili ai soli soggetti riceventi (in caso di più utenze), oppure potranno essere visibili solo al soggetto ricevente che li ha caricati. Grazie a questa nuova funzionalità i soggetti riceventi potranno mantenere evidenze delle proprie attività di accertamento sulla piattaforma, senza necessariamente condividerle con il segnalante.

- Il secondo aggiornamento introduce una funzionalità che aumenta il livello di personalizzazione della piattaforma con la possibilità di caricare collegamenti a policy dell'ente o dell'organizzazione, in particolare in relazione a: procedura di gestione delle segnalazioni (di whistleblowing), informativa privacy e dichiarazione di accessibilità. L'inserimento di questi link può essere fatto direttamente dall'ente nella sezione "Impostazioni". Il segnalante potrà dunque avere presente il riferimento alla documentazione predisposta dall'ente in tema di whistleblowing anche mentre sta compilando una segnalazione.

- Infine, i questionari per le versioni standard WB-PA, WB-SCP e WB-ORG sono stati migliorati e aggiornati in linea con la normativa.

4.2.3 Canale ORALE

Solo se richiesto dal segnalante, la segnalazione può essere acquisita o integrata mediante incontro diretto. In tale ultimo caso, le misure di sicurezza di tipo organizzativo sono innanzitutto una attenta programmazione della formazione sulla procedura dell'intero personale dell'Ente, il quale deve essere addestrato in caso di richiesta di incontro, a tenere un comportamento volto alla riservatezza e discrezionalità necessarie anche per gestire l'incontro che si terrà alla presenza di RPCT e verrà tenuto all'interno dell'Ente, in locale chiuso e con adeguate misure di sicurezza di tipo fisico. L'incontro verrà verbalizzato. Saranno concordati i tempi e le modalità dello stesso. La dinamica di interazione sarà sotto forma di domande dell'RPCT e risposte del segnalante. Al termine dell'incontro sarà sottoscritto il verbale della segnalazione, che verrà custodito dall'RPCT in modalità riservata e in cassetto dotato di chiusura a chiave.

Tramite la segnalazione orale, la tutela della identità personale del segnalante può risultare in concreto più debole a causa della sua stessa natura, che impone la presenza fisica del segnalante, presso i locali dell'Ente, per cui la segnalazione informatica mediante piattaforma è suggerita in via prioritaria.

A rigore la normativa richiede l'apertura di un canale orale mediante una linea telefonica o sistema di messaggistica vocale dedicato), al momento l'Ente ha scelto di non utilizzare questo canale.

5. RACCOMANDAZIONE E AZIONI DI MIGLIORAMENTO

5.1 Azioni raccomandate alla luce della valutazione dei rischi e dall'analisi della procedura adottata dall'Ente.

Sono fortemente consigliate in sintesi le seguenti azioni:

1. Tutti i dipendenti e i consiglieri che accedono al sistema di whistleblowing dovrebbero partecipare ad attività formative periodiche che trattano le tematiche di sicurezza e protezione dei dati personali.

2. L'Ente dovrebbe attenzionare, con l'aiuto del proprio ADS il secondo aggiornamento della piattaforma sopra descritto che introduce una funzionalità che aumenta il livello di personalizzazione della piattaforma con la possibilità di caricare collegamenti a policy dell'ente o dell'organizzazione, in particolare in relazione a: procedura di gestione delle segnalazioni (di whistleblowing), informativa privacy e dichiarazione di accessibilità. L'inserimento di questi link può essere fatto direttamente dall'ente nella sezione "Impostazioni" permettendo al segnalante di avere il riferimento alla documentazione predisposta dall'ente in tema di whistleblowing anche mentre sta compilando una segnalazione.
3. Nella pagina sul whistleblowing è opportuno che gli utenti siano messi a conoscenza, oltre che dei riferimenti normativi, anche delle seguenti informazioni:

    - i canali alternativi disponibili per inviare una segnalazione interna, oltre alla piattaforma WhistleblowingPA;
    - i presupposti per poter inviare una segnalazione interna;
    - l'elenco di tutti i soggetti che possono inviare una segnalazione;
    - il destinatario o i destinatari delle segnalazioni all'interno dell'ente o organizzazione;
    - le tutele previste per coloro che decidono di inviare una segnalazione;
    - cosa può essere oggetto della segnalazione interna;
    - le procedure e modalità di gestione delle segnalazioni, della trasmissione delle informazioni, del trattamento e della conservazione dei dati personali;
    - le conseguenze in caso di abuso o di uso strumentale dello strumento del whistleblowing;
    - i canali, le procedure e i presupposti per effettuare una segnalazione all'esterno dell'ente o dell'organizzazione.

4. L'Ente dovrebbe garantire, ove possibile, il tracciamento dell'attività del personale autorizzato nel rispetto delle garanzie a tutela del segnalante.

5. Dato l'avvicendamento della figura del RPCT, l'Ente deve garantire la disattivazione delle credenziali di autenticazione assegnate al RPCT in seguito alle sue dimissioni.

6. L'aggiornamento del registro delle attività di trattamento di cui all'art.30 del GDPR inserendo la procedura e la DPIA.

Allegati

1. Procedura per la gestione delle segnalazioni di condotte illecite o di irregolarità conosciute in ragione del servizio e relativo
2. Informativa art. 13 GDPR
3. Modello di segnalazione, comunicazione di avvio procedimento ed esito di procedimento (Whistleblowing)
4. Tabella di valutazione dei rischi

L'Ordine dei Medici di Perugia

avv. Alexander Cassisa

Questo lavoro è stato eseguito con la collaborazione del DPO dell'Ente che esprime parere positivo sulla presente DPIA

avv. Silvia Boschello