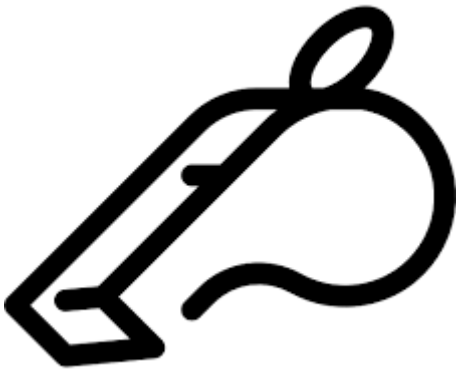
Valutazione d'impatto sulla protezione dei dati (cd. DPIA) ex art. 35 GDPR

Trattamento oggetto della DPIA

Whistleblowing



Titolare del Trattamento

Ordine dei Tecnici Sanitari di Radiologia Medica e delle Professioni Sanitarie Tecniche, della Riabilitazione e della Prevenzione delle Province di Gorizia Pordenone Trieste Udine (C.F. 94079620301)

Nome validatore /DPO

Match di Massimo Giuriati & C. S.a.s. (P.IVA 03865860278)

Data di creazione

In attuazione della Direttiva (UE) 2019/1937, è stato emanato il **D.lgs. n. 24 del 10 marzo 2023**, 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", del quale si richiamano le seguenti norme

Art. 2 *Definizioni*

1. Ai fini del presente decreto, si intendono per:

a) «violazioni»: comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che consistono in:

1) illeciti amministrativi, contabili, civili o penali che non rientrano nei numeri 3), 4), 5) e 6);

2) condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n. 231, o violazioni dei modelli di organizzazione e gestione ivi previsti, che non rientrano nei numeri 3), 4), 5) e 6);

3) illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali indicati nell'allegato al presente decreto ovvero degli atti nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nell' allegato alla direttiva (UE) 2019/1937, seppur non indicati nell'allegato al presente decreto, relativi ai seguenti settori: appalti 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;

4) atti od omissioni che ledono gli interessi finanziari dell'Unione di cui all'articolo 325 del Trattato sul funzionamento dell'Unione europea specificati nel diritto derivato pertinente dell'Unione europea;

5) atti od omissioni riguardanti il mercato interno, di cui all' articolo 26, paragrafo 2, del Trattato sul funzionamento dell'Unione europea, comprese le violazioni delle norme dell'Unione europea in materia di concorrenza e di aiuti di Stato, nonché le violazioni riguardanti il mercato interno connesse ad atti che violano le norme in materia di imposta sulle società o i meccanismi il cui fi ne è ottenere un vantaggio fi scale che vanifica l'oggetto o la finalità della normativa applicabile in materia di imposta sulle società;

6) atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione nei settori indicati nei numeri 3), 4) e 5);

b) **«informazioni sulle violazioni»**: informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni;

c) **«segnalazione» o «segnalare»**: la comunicazione scritta od orale di informazioni sulle violazioni;

d) **«segnalazione interna»**: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione interna di cui all'articolo 4;

e) **«segnalazione esterna»**: la comunicazione, scritta od orale, delle informazioni sulle violazioni, presentata tramite il canale di segnalazione esterna di cui all'articolo 7;

f) **«divulgazione pubblica» o «divulgare pubblicamente»**: 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;

g) **«persona segnalante»**: la persona fi sica che effettua la segnalazione o la divulgazione pubblica di informazioni sulle violazioni acquisite nell'ambito del proprio contesto lavorativo;

h) **«facilitatore»**: una persona fi sica che assiste una persona segnalante nel processo di segnalazione, operante all'interno del medesimo contesto lavorativo e la cui assistenza deve essere mantenuta riservata;

i) **«contesto lavorativo»**: le attività lavorative o professionali, presenti passate, svolte nell'ambito dei rapporti di cui all'articolo 3, commi 3 o 4, attraverso le quali, indipendentemente dalla natura di tali attività, una persona acquisisce informazioni sulle violazioni e nel cui ambito potrebbe rischiare di subire ritorsioni in caso di segnalazione o di divulgazione pubblica o di denuncia all'autorità giudiziaria o contabile;

l) **«persona coinvolta»**: la persona fi sica o giuridica menzionata nella segnalazione interna o esterna ovvero nella divulgazione pubblica come persona alla quale la violazione è attribuita o come persona comunque implicata nella violazione segnalata o divulgata pubblicamente;

m) **«ritorsione»**: qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all'autorità giudiziaria o contabile o della divulgazione pubblica che provoca o può provocare alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto;

n) **«seguito»**: l'azione intrapresa dal soggetto cui è affidata la gestione del canale di segnalazione per valutare la sussistenza dei fatti segnalati, l'esito delle indagini e le eventuali misure adottate;

o) **«riscontro»**: comunicazione alla persona segnalante di informazioni relative al seguito che viene dato o che si intende dare alla segnalazione;

p) **«soggetti del settore pubblico»**: le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, le autorità amministrative indipendenti di garanzia, vigilanza o regolazione, gli enti pubblici economici, gli organismi di diritto pubblico di cui all'articolo 3,comma 1, lettera d), del decreto legislativo 18 aprile 2016, n. 50, i concessionari di pubblico servizio, le società a controllo pubblico e le società in house, così come definite, rispettivamente, dall'articolo 2, comma1, lettere m) e o), del decreto legislativo 19 agosto 2016, n. 175, anche se quotate;

q) **«soggetti del settore privato»**: soggetti, diversi da quelli rientranti nella definizione di soggetti del settore pubblico, i quali:

1) hanno impiegato, nell'ultimo anno, la media di almeno cinquanta lavoratori subordinati con contratti di lavoro a tempo indeterminato o determinato;

2) rientrano nell'ambito di applicazione degli atti dell'Unione di cui alle parti I.B e II dell'allegato, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1);

3) sono diversi dai soggetti di cui al numero 2), rientrano nell'ambito di applicazione del decreto legislativo 8 giugno 2001, n. 231, e adottano modelli di organizzazione e gestione ivi previsti, anche se nell'ultimo anno non hanno raggiunto la media di lavoratori subordinati di cui al numero 1).

Articolo 13 *Trattamento dei dati personali*

1. Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE) 2018/1725.

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

3. I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

4. I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4, in qualità di titolari del trattamento, nel rispetto dei principi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

5. I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.

6. 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.

Valutazione d'impatto sulla protezione dei dati e consultazione preventiva (GDPR)

Articolo 35 *Valutazione d'impatto sulla protezione dei dati*

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;

b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o

c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;

b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;

c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e

d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10. Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

Articolo 36 *Consultazione preventiva*

1. Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.

2. Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

3. Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo:

a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;

b) le finalità e i mezzi del trattamento previsto;

c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento;

d) ove applicabile, i dati di contatto del responsabile della protezione dei dati;

e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; e

f) ogni altra informazione richiesta dall'autorità di controllo.

4. Gli Stati membri consultano l'autorità di controllo durante l'elaborazione di una proposta di atto legislativo che deve essere adottato dai parlamenti nazionali o di misura regolamentare basata su detto atto legislativo relativamente al trattamento.

5. Nonostante il paragrafo 1, il diritto degli Stati membri può prescrivere che i titolari del trattamento consultino l'autorità di controllo, e ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica.

I Contesto

1. Panoramica del trattamento

La presente valutazione di impatto si compone di nr. 3 allegati:

01) Informativa trattamento dati personali;
02) Modalità di conservazione delle chiavi crittografiche del fornitore Whistleblowing PA;
03) Documentazione a supporto del titolare nella valutazione d'impatto sulla protezione dei dati del fornitore Whistleblowing PA.

Quale è il trattamento in considerazione?

Il presente trattamento ha ad oggetto la gestione delle segnalazioni ad opera dei segnalanti di violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica, di cui siano venuti a conoscenza in un contesto lavorativo pubblico (art. 1, comma 1, D.lgs. n. 24/2023).

Quali sono le responsabilità connesse al trattamento?

1.1.1. Obblighi normativamente imposti

Il Titolare del trattamento, sentite le rappresentanze o le organizzazioni sindacali di cui all' articolo 51 del decreto legislativo n. 81 del 2015, attiva, ai sensi dell'art. 4 D.lgs. n 24/2023, propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione (art. 6, par. 1, lett. c), Reg. UE 2016/679).

Sanzioni previste per l'inadempimento

L'inottemperanza ai suddetti obblighi può comportare le sanzioni previste dalla normativa di settore in materia di trattamento dati, nonché le sanzioni di cui all'art. 21 D.lgs. n 24/2023.
Restano impregiudicate le sanzioni amministrative e penali rispettivamente previste dal Regolamento UE 2016/679 e dal Codice Privacy in capo al Titolare del trattamento.

1.2. Ci sono standard applicabili al trattamento?

Le Linee Guida ANAC, approvate con Delibera n. 311 del 12 luglio 2023, forniscono un utile ed autorevole indirizzo da considerare nel trattamento delle segnalazioni.
In quanto Ente pubblico deve inoltre aversi riguardo alle Linee Guida AGID in materia di organizzazione dell'Ente e gestionale.

2. Dati, processi e risorse di supporto

2.1. Quali sono i dati trattati?

I dati trattati sono dati personali comuni e dati relativi a reati ex art. 10 Reg. UE 2016/679.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

2.2. Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

I dati vengono acquisiti attraverso il canale di segnalazione interno; tuttavia, i segnalanti possono procedere alla segnalazione altresì attraverso:

- Canale esterno (ANAC);

- Divulgazione pubblica (tramite stampa, mezzi elettronici o mezzi di diffusione in grado di raggiungere un numero elevato di persone);
- Denuncia all'Autorità giudiziaria o contabile.

I dipendenti vengono informati della procedura interna e dei possibili canali di segnalazione. Le segnalazioni sono archiviate nel server dell'Ente e, secondo le modalità descritte negli allegati 2-3 della presente DPIA, anche nei server del fornitore del servizio Whistleblowing P.A. Compete al responsabile esterno (fornitore) la conservazione delle chiavi necessarie per decrittare le informazioni presenti sulla Piattaforma.
Come disposto dall'art. 14 D.lgs. n. 24/2023:
"1. Le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.
2. Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale. In caso di trascrizione, la persona segnalante può verificare, rettificare o confermare il contenuto della trascrizione mediante la propria sottoscrizione.
3. Se per la segnalazione si utilizza una linea telefonica non registrata o un altro sistema di messaggistica vocale non registrato la segnalazione è documentata per iscritto mediante resoconto dettagliato della conversazione cura del personale addetto. La persona segnalante può verificare, rettificare e confermare il contenuto della trascrizione mediante la propria sottoscrizione.
4. Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione."

2.3. Quali sono le risorse di supporto ai dati?

Le risorse informatiche dell'Ente sono censite nel registro del Titolare, unitamente alle relative misure di sicurezza. Il titolare utilizza Google Drive come soluzione cloud.
La piattaforma Whistleblowing PA, basata sul software GlobaLeaks (https://www.globaleaks.org/it/), di cui il Titolare si avvale, permette al Responsabile della prevenzione della corruzione e della trasparenza (RPCT) di ricevere le segnalazioni di illeciti da parte dei dipendenti dell'Ente e di dialogare con i segnalanti, anche in modo anonimo.
In particolare, l'utilizzo di un protocollo di crittografia garantisce la protezione dei dati identificativi dell'identità del segnalante, mentre il codice identificativo univoco ottenuto a seguito della segnalazione registrata su questo portale consente al segnalante di "dialogare" con il Titolare in modo anonimo e spersonalizzato. Quanto alle modalità di separazione e conservazione delle chiavi di crittografia si rimanda all'allegato 3.
Grazie all'utilizzo di questo protocollo il livello di riservatezza è dunque massimo.
Per quanto riguarda le specifiche tecniche si rimanda agli allegati 2 e 3 della presente DPIA.

II. Principi Fondamentali

1. Proporzionalità e necessità

1.1. Gli scopi del trattamento sono specifici, espliciti e legittimi?

I legittimi scopi del trattamento sono specificamente individuati nella prevenzione e accertamento delle violazioni di cui all'art 2, lett. a), D.lgs. n. 24/2023.
Gli scopi sono esplicitati nelle informative messe a disposizione dei dipendenti e nelle specifiche procedure.
Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse (art. 12, comma 1, D.lgs. n. 24/2023).

1.2. Quali sono le basi legali che rendono lecito il trattamento?

La legittimità del trattamento è determinata dall'adempimento di obblighi legali ai quali è soggetto il Titolare del trattamento (D.lgs. n. 24/2023; art. 6, par. 1, lett. c), Reg. UE 2016/679).

1.3. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Ogni trattamento dei dati personali è effettuato nel rispetto dei principi di cui all'art 5 Reg. UE 2016/679.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente (art. 13, comma 2, D.lgs. n. 24/2023).

1.4. I dati sono esatti e aggiornati?

I dati personali sono trattati nel rispetto dell'art. 5, par. 1, lett. d), Reg. UE 2016/679, i cui principi sono declinati nella procedura whistleblowing adottata dal Titolare.

1.5. Qual è il periodo di conservazione dei dati?

In conformità all'art. 14 D.lgs. n. 24/2023, i dati vengono conservati "*per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del presente decreto e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.*"

2. Misure a tutela dei diritti degli interessati

2.1. Come sono informati del trattamento gli interessati?

Si premette che con "interessati" si intendono i soggetti segnalanti e quelli interessati dalla specifica procedura.
Agli interessati viene messa a disposizione specifica informativa.
Inoltre, gli interessati vengono informati, mediante affissione in bacheca dell'ente, della procedura interna per la gestione dei canali di segnalazione di cui all'art. D.lgs. n. 24/2023.

2.2. Ove applicabile: come si ottiene il consenso degli interessati?

Il presente trattamento ha come base giuridica l'adempimento di obblighi legali ai quali è soggetto il Titolare del trattamento (D.lgs. n. 24/2023; art. 6, par. 1, lett. c), Reg. UE 2016/679).
Tuttavia, il consenso espresso della persona segnalante può rilevare ai sensi dell'art. 12, comma 2, D.lgs. n. 24/2023, secondo cui: *"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, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196".

Il consenso dell'interessato dovrà essere manifestato e raccolto successivamente in conformità al Reg. UE 2016/679.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Ai sensi dell'art. 13 D.lgs. n. 24/2023, i diritti di cui agli artt. 15 – 22 Reg. UE 2016/679 possono essere esercitati nei limiti di quanto previsto dall'art. 2-undecies D.lgs. n. 196/2003.

2.4. Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Ai sensi dell'art. 13 D.lgs. n. 24/2023, i diritti di cui agli artt. 15 – 22 Reg. UE 2016/679 possono essere esercitati nei limiti di quanto previsto dall'art. 2-undecies D.lgs. n. 196/2003. Il tutto comunicando con il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) e con il Responsabile della protezione dei dati.

2.5. Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Ai sensi dell'art. 13 D.lgs. n. 24/2023, i diritti di cui agli artt. 15 – 22 Reg. UE 2016/679 possono essere esercitati nei limiti di quanto previsto dall'art. 2-undecies D.lgs. n. 196/2003. Il tutto comunicando con il Responsabile della prevenzione della corruzione e della trasparenza (RPCT) e con il Responsabile della protezione dei dati.

2.6. Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

La società a cui è stato affidato il servizio di gestione del canale di segnalazione è Whistleblowing PA di Transparency International Italia e Whistleblowing Solutions I.S. S.r.l., (C.F. e P. IVA 09495830961), nominata responsabile del trattamento ex art. 28 Reg. UE 2016/679.

2.7. In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

N.A.

III. Rischi

1. Accesso illegittimo ai dati

1.1 Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

La perdita di riservatezza dei dati personali degli interessati potrebbe esporre quest'ultimi a subire atti ritorsivi, in conseguenza delle segnalazioni.

1.2. Quali sono le principali minacce[1] che potrebbero concretizzare il rischio?

Errata applicazione delle procedure interne; errato settaggio delle risorse informatiche e distribuzione degli accessi; sistema di criptazione non conforme; data breach.

1.3 Quali sono le fonti di rischio[2]?

Fonti umane interne:	In astratto concretamente ipotizzabile	Nemmeno in astratto concretamente ipotizzabile
- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.	Il rischio è ipotizzabile, specie per mano di dipendente negligente che diffonda informazioni, contenute nelle segnalazioni	
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.		Non è prevista interazione di alcun utente nel trattamento in oggetto.
Fonti umane esterne		
- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio	Il rischio è ipotizzabile, specie in punto diffusione di informazioni, contenute nelle segnalazioni	
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo	Il rischio è ipotizzabile, specie in punto diffusione di informazioni, contenute nelle segnalazioni	

[1] **Minaccia:** Modalità operativa comprendente una o più azioni individuali sulle risorse che supportano i dati. La minaccia può essere utilizzata, intenzionalmente o meno, da fonti di rischio e può quindi causare un evento pericoloso.

[2] **Fonte di rischio:** Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.

- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine	Ipotesi astrattamente applicabile avendo riguardo all'esistenza di un fornitore esterno, sebbene le misure di sicurezza siano adeguate.	
- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.	Ipotesi astrattamente applicabile avendo riguardo all'esistenza di un fornitore esterno, sebbene le misure di sicurezza siano adeguate.	
Fonti non umane		
interruzione di corrente		L'ipotesi non appare attinente al rischio in oggetto
incendio/cataclisma naturale		L'ipotesi non appare attinente al rischio in oggetto
Interruzione della linea dati		L'ipotesi non appare attinente al rischio in oggetto
Rovina dell'edificio	x	L'ipotesi non appare attinente al rischio in oggetto

1.4 Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

(Resta fermo quanto specificato agli allegati 2-3 della presente Dpia)

	Fonti di rischio: ACCESSO ILLEGITTIMO AI DATI (Misure in essere) (misure da implementare- vulnerabilità rilevata-)			
CHECK MISURE DI MITIGAZIONE DEL RISCHIO	FONTI UMANE ESTERNE	FONTI UMANE INTERNE	FONTI NON UMANE	ANNOTAZIONE VULNERABILITA' RESIDUA
	MISURE ORGANIZZATIVE			
E' stato designato il referente per la gestione dei canali di segnalazione?	N/A	RPCT come per legge	N/A	N/A
Sono state stabilite le modalità di archiviazione delle segnalazioni?	E' stato predisposto il registro data breach. E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6 mesi a verifica degli accessi.	E' stata predisposto il registro data breach E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6 mesi a verifica degli accessi..	E' stata predisposto il registro data breach. E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6 mesi a verifica degli accessi.	N/A
E' stato stabilito chi deve sottoporsi a formazione specifica e quando?	N/A	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A
E' stato stabilito chi può avere accesso alla segnalazioni ed a quali scopi?	Procedura whistleblowing	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A

Sono state implementate le procedure operative, tra cui quella in caso di data breach?	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	N/A
Sono state individuate le procedure che i terzi devono seguire per ottenere copia delle segnalazioni, così come le procedure per decidere se negare o accordare tali richieste?	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime.	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime.	N/A	N/A
Sono state individuate le procedure per selezionare i fornitori del sistema dei canali di segnalazione?	L'Ente ha sottoscritto con la ditta un capitolato tecnico che assicura il rispetto degli standard ISO27001 / ISO27017 / ISO27018 / Qualifica AGID / Certificazione CSA Star	N/A	N/A	N/A
Sono state individuate le procedure per la gestione degli incidenti e procedure di disaster recovery?	Procedura data breach formalizzata	Procedura data breach formalizzata	Procedura data breach formalizzata	
	MISURE TECNICHE			
	Si rinvia agli allegati 2 e 3.			

1.5 Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel trattamento dei dati personali", DICEMBRE 2017, tabella in calce, il rischio, al netto delle misure di contenimento deve essere quantificato come ad impatto **potenziale alto.**

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Invero gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (subire atti ritorsivi, con conseguente stress psicologico, ecc.). Eventuale diffusione delle informazioni delle segnalazioni, specie nel web, possono aumentare la probabilità per gli interessati di essere vittime di reati ad opera di soggetti od organizzazioni criminali, i cui interessi possano essere pregiudicati dalle segnalazioni.

1.6. Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel trattamento dei dati personali", DICEMBRE 2017, tabella in calce, la probabilità del rischio, in relazione alle misure di mitigazione del rischio sopra elencate deve essere quantificato come **Bassa**: le misure di contenimento individuate appaiono idonee a contenere il rischio, e questo anche alla luce dell'assenza di precedenti interni specifici.

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

2. Modifiche indesiderate dei dati

2.1. Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Le modifiche indesiderate dei dati personali dell'interessato potrebbero comportare l'impossibilità, o quantomeno difficoltà, a risalire all'identità del segnalante, con conseguenti problematiche nel dare seguito alla segnalazione effettuata, con possibile prosecuzione della violazione oggetto della segnalazione medesima.
Il Titolare del trattamento potrebbe, pertanto, non garantire una conforme gestione del canale di segnalazione, in violazione dell'art. 5 D.lgs. n. 24/2023: mancato o tardivo rilascio alla persona segnalante dell'avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione; mancate o tardive interlocuzioni con la persona segnalante; mancato o tardivo seguito alle segnalazioni; mancato riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento, ecc.).

2.2. Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Errata applicazione delle procedure interne; conservazione dei dati non conforme.

2.3. Quali sono le fonti di rischio?

Fonti umane interne:	In astratto concretamente ipotizzabile	Nemmeno in astratto concretamente ipotizzabile
- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.	Il rischio è ipotizzabile, specie per mano di dipendente negligente che modifichi o non provveda alla conforme conservazione delle informazioni, contenute nelle segnalazioni	
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.		Non è prevista interazione di alcun utente nel trattamento in oggetto.
Fonti umane esterne		

- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio	Il rischio è ipotizzabile, specie in punto di modifica di informazioni, contenute nelle segnalazioni	
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo	Il rischio è ipotizzabile, specie in punto di modifica di informazioni, contenute nelle segnalazioni	
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine	Ipotesi astrattamente applicabile avendo riguardo all'esistenza di un fornitore esterno, sebbene le misure di sicurezza siano adeguate.	
- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.	Ipotesi astrattamente applicabile avendo riguardo all'esistenza di un fornitore esterno, sebbene le misure di sicurezza siano adeguate.	
Fonti non umane		
interruzione di corrente		L'ipotesi non appare attinente al rischio in oggetto
incendio/cataclisma naturale		L'ipotesi non appare attinente al rischio in oggetto
Interruzione della linea dati		L'ipotesi non appare attinente al rischio in oggetto
Rovina dell'edificio	x	L'ipotesi non appare attinente al rischio in oggetto

2.4.Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

(Resta fermo quanto specificato negli allegati 2 e 3 della presente DPIA)

	Fonti di rischio: MODIFICHE INDESIDERATE DEI DATI (Misure in essere) (misure da implementare- vulnerabilità rilevata-)			
CHECK MISURE DI MITIGAZIONE DEL RISCHIO	FONTI UMANE ESTERNE	FONTI UMANE INTERNE	FONTI NON UMANE	ANNOTAZIONE VULNERABILITA' RESIDUA
	MISURE ORGANIZZATIVE			
E' stato designato il referente per la gestione dei canali di segnalazione?	N/A	RPCT come per legge	N/A	N/A
Sono state stabilite le modalità di archiviazione delle segnalazioni?	E' stato predisposto il registro data breach. E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6 mesi a verifica degli accessi.	E' stato predisposto il registro data breach. E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6 mesi a verifica degli accessi.	E' stato predisposto il registro data breach. E' stata settata la durata della conservazione delle segnalazioni, nonché un sistema di file log immutabile per 6	N/A

			mesi a verifica degli accessi.	
E' stato stabilito chi deve sottoporsi a formazione specifica e quando?	N/A	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A
E' stato stabilito chi può avere accesso alla segnalazioni ed a quali scopi?	Esistenza di regolamento informatico e soggetti autorizzati ex art. 29 Gdpr.	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A
Sono state implementate le procedure operative, tra cui quella in caso di data breach?	E' stata predisposta una procedura data breach, implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach, implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach, implementata come procedura dell'Ente.	N/A
Sono state individuate le procedure che i terzi devono seguire per ottenere copia delle segnalazioni, così come le procedure per decidere se negare o accordare tali richieste?	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime. La segnalazione è sottratta all'accesso previsto dagli artt. 22 ss. L. 241/90 e dagli artt. 5 ss. D.lgs. n. 33/2013.	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime. La segnalazione è sottratta all'accesso previsto dagli artt. 22 ss. L. 241/90 e dagli artt. 5 ss. D.lgs. n. 33/2013.	N/A	N/A
Sono state individuate le procedure per selezionare i fornitori del sistema dei canali di segnalazione?	L'Ente ha sottoscritto con la ditta un capitolato tecnico che assicura il rispetto degli standard ISO27001 / ISO27017 / ISO27018 / Qualifica AGID / Certificazione CSA Star	N/A	N/A	N/A
Sono state individuate le procedure per la gestione degli incidenti e procedure di disaster recovery?	Procedura data breach formalizzata	Procedura data breach formalizzata	Procedura data breach formalizzata	
	MISURE TECNICHE			
	Si rinvia all'allegato.			

2.5. Come stimereste la gravità del rischio?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel trattamento dei dati personali", DICEMBRE 2017, tabella in calce, il rischio, al netto delle misure di contenimento deve essere quantificato come ad impatto **potenziale medio.**

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Invero gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare nonostante alcune difficoltà (maggiore attesa nel ricevere riscontro alla segnalazione effettuata, necessità di effettuare nuovamente la segnalazione, ecc.). La modifica dei dati personali, comportando un'impossibilità o difficoltà nell'identificare il segnalante, potrebbe favorire la continuazione della violazione oggetto della segnalazione, eventualmente a danno della persona segnalante stessa.

2.6. Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel trattamento dei dati personali", DICEMBRE 2017, tabella in calce, la probabilità del rischio, in relazione alla misure di mitigazione del rischio sopra elencate deve essere quantificato come **Bassa**: le misure di contenimento individuate appaiono idonee a contenere il rischio, e questo anche alla luce dell'assenza di precedenti interni specifici.

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

3. Perdita di dati

3.1. Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

La perdita dei dati contenuti nelle segnalazioni potrebbe comportare l'impossibilità, o quantomeno difficoltà, a risalire all'identità del segnalante, con conseguenti problematiche nel dare seguito alla segnalazione effettuata, con possibile prosecuzione della violazione oggetto della segnalazione medesima.

Il Titolare del trattamento potrebbe, pertanto, non garantire una conforme gestione del canale di segnalazione, in violazione dell'art. 5 D.lgs. n. 24/2023: mancato o tardivo rilascio alla persona segnalante dell'avviso di ricevimento della segnalazione entro sette giorni dalla data di ricezione; mancate o tardive interlocuzioni con la persona segnalante; mancato o tardivo seguito alle

segnalazioni; mancato riscontro alla segnalazione entro tre mesi dalla data dell'avviso di ricevimento, ecc.
La perdita delle informazioni comporterebbe altresì la perdita di potenziali elementi probatori in sede giudiziale o in controversie extragiudiziali, mancata attivazione delle Autorità competenti, mancata tutela alle persone segnalanti e ai soggetti di cui all'art. 3, comma 5, lett. a), b), c), d), D.lgs. n. 24/2023.

3.2. Quali sono le principali minacce che potrebbero concretizzare il rischio?

Errata applicazione delle procedure interne; errato settaggio delle risorse informatiche e distribuzione degli accessi; errato posizionamento del DVR in area non sicura; mancata protezione del dispositivo di archiviazione.

3.3. Quali sono le fonti di rischio?

Fonti umane interne:	In astratto concretamente ipotizzabile	Nemmeno in astratto concretamente ipotizzabile
- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.	Il rischio potrebbe ipotizzarsi come concorso per la copertura di un fatto illecito al fine di distruggere eventuali fonti di prova	
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.	Il rischio potrebbe ipotizzarsi come concorso per la copertura di un fatto illecito al fine di distruggere eventuali fonti di prova	
Fonti umane esterne		
- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio	Il rischio potrebbe ipotizzarsi come concorso per la copertura di un fatto illecito al fine di distruggere eventuali fonti di prova	
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo	Il rischio è ipotizzabile, specie in punto di perdita di informazioni, contenute nelle segnalazioni	
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine	Il rischio è ipotizzabile, specie in punto di perdita di informazioni, contenute nelle segnalazioni	

- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni.	Il rischio è ipotizzabile, specie in punto di perdita di informazioni, contenute nelle segnalazioni	
Fonti non umane		
interruzione di corrente	Per quanto sussistano generatori di emergenza breve interruzioni sono inevitabili	
incendio/cataclisma naturale	L'Ente ha sottoscritto con la ditta un capitolato tecnico che assicura il rispetto degli standard ISO27001 / ISO27017 / ISO27018 / Qualifica AGID / Certificazione CSA Star che mitiga i rischi derivanti da fonti non umane	
Interruzione della linea dati	L'Ente ha sottoscritto con la ditta un capitolato tecnico che assicura il rispetto degli standard ISO27001 / ISO27017 / ISO27018 / Qualifica AGID / Certificazione CSA Star che mitiga i rischi derivanti da fonti non umane	
Rovina dell'edificio	L'Ente ha sottoscritto con la ditta un capitolato tecnico che assicura il rispetto degli standard ISO27001 / ISO27017 / ISO27018 / Qualifica AGID / Certificazione CSA Star che mitiga i rischi derivanti da fonti non umane	

3.4. Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

	Fonti di rischio: PERDITA DEI DATI (Misure in essere) (misure da implementare- vulnerabilità rilevata-)			
CHECK MISURE DI MITIGAZIONE DEL RISCHIO	FONTI UMANE ESTERNE	FONTI UMANE INTERNE	FONTI NON UMANE	ANNOTAZIONE VULNERABILITA' RESIDUA
	MISURE ORGANIZZATIVE			
E' stato designato il referente per la gestione dei canali di segnalazione?	N/A	RPCT come per legge	N/A	N/A
Sono state stabilite le modalità di registrazione dei video e la durata, includendo gli archivi dei video riguardanti incidenti sulla sicurezza?	N/A	N/A	N/A	N/A
E' stato stabilito chi deve sottoporsi a formazione specifica e quando?	N/A	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A

E' stato stabilito chi può avere accesso alla segnalazioni ed a quali scopi?	Esistenza di regolamento informatico e soggetti autorizzati ex art. 29 Gdpr.	Sono stati individuati i soggetti autorizzati e adeguatamente formati.	N/A	N/A
Sono state implementate le procedure operative, tra cui quella in caso di data breach?	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	E' stata predisposta una procedura data breach implementata come procedura dell'Ente.	N/A
Sono state individuate le procedure che i terzi devono seguire per ottenere copia delle registrazioni, così come le procedure per decidere se negare o accordare tali richieste?	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime.	E' stata individuata una procedura per l'esercizio dei diritti degli interessati, onde prevenire le richieste illegittime.	N/A	N/A
Sono state individuate le procedure per la gestione degli incidenti e procedure di disaster recovery?	Si rinvia alle specifiche tecniche degli allegati 2-3	Si rinvia alle specifiche tecniche degli allegati 2-3	Si rinvia alle specifiche tecniche degli allegati 2-3	
	MISURE TECNICHE			
	Sicurezza fisica			
	Si rinvia alle specifiche tecniche degli allegati 2-3 in relazione al software whistleblowing autorizzato.			

3.6. Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel trattamento dei dati personali", DICEMBRE 2017, tabella in calce, il rischio, al netto delle misure di contenimento deve essere quantificato come ad impatto **potenziale alto.**

LIVELLO DI IMPATTO	DESCRIZIONE
Basso	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).
Medio	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.).
Alto	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.).
Molto alto	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.).

Invero gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (stress psicologico e danni conseguenti al perpetrarsi delle violazioni). La perdita delle informazioni contenute nelle segnalazioni può comportare l'inutilizzabilità di elementi probatori in sede giudiziale o extragiudiziale, anche a tutela dei diritti dei segnalanti; mancata attivazione delle Autorità competente; mancata tutela della persona segnalante da atti di ritorsione, ecc.

3.7. Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Secondo la definizione fornite da Enisa nel documento "Manuale sulla Sicurezza nel

trattamento dei dati personali", DICEMBRE 2017, tabella in calce, la probabilità del rischio, in relazione alle misure di mitigazione del rischio sopra elencate deve essere quantificato come **Bassa**: le misure di contenimento individuate appaiono idonee a contenere il rischio, agendo sia sugli asset umani che sugli asset informatici/fisici, e questo anche alla luce dell'assenza di precedenti interni specifici.

- Basso: è improbabile che la minaccia si materializzi.
- Medio: c'è una ragionevole possibilità che la minaccia si materializzi.
- Alto: la minaccia potrebbe materializzarsi.

IV. Valutazione di chiusura

Alla luce della DPIA in oggetto è possibile trarre le seguenti valutazioni di sintesi:

	Gravità del Rischio al netto delle misure di contenimento	Probabilità del Rischio alla luce delle misure di contenimento	Vulnerabilità residue rilevate?
Accesso illegittimo ai dati			N/A
Modifiche indesiderate dei dati			N/A
Perdita dei dati			N/A

	Molto alto
	Alto
	Medio
	Basso

Alla luce della vulnerabilità residue e della gravità del rischio potenziale per gli interessati all'esito della DPIA si ritiene

- ■ La sussistenza delle condizioni per procedere al trattamento in oggetto.
- □ Necessaria l'adozione di ulteriori misure di contenimento per mitigare il rischio prima di procedere il trattamento, specie alla luce delle vulnerabilità rilevate
- □ Necessario procedere a consultazione preventiva ex art. 36 GDPR stante l'impossibilità dell'opzione precedente.

Luogo e Data.
Tavagnacco, 31 gennaio 2024