Camera di Commercio
Cuneo

D.P.I.A. EX ART. 35 GDPR

CCIAA CUNEO

GESTIONE SEGNALAZIONI CONDOTTE ILLECITE C.D. WHISTLEBLOWING

Inseritore: Referente interno privacy	**Data di inizio**: maggio 2024
Revisore: RPCT	**Data di conclusione:** maggio 2029
Validatore: Segretario Generale	
Allegati:	
All.1 Documentazione a supporto del titolare per la valutazione di impatto sulla protezione dei dati	
All. 2 Nomina del Responsabile esterno del Trattamento	

SOMMARIO

1 Contesto

Questa sezione permette una visione complessiva del trattamento o del processo sottoposto a DPIA.

1.1 Ambito di attività del Titolare del trattamento

La Camera di Commercio, industria, artigianato e agricoltura di Cuneo, di seguito “Camera di commercio”, è un ente pubblico dotato di autonomia funzionale che svolge, nell'ambito della circoscrizione territoriale di competenza, sulla base del principio di sussidiarietà di cui all'articolo 118 della Costituzione, funzioni di interesse generale per il sistema delle imprese, curandone lo sviluppo nell'ambito delle economie locali.
I compiti e le funzioni sono definite dall’art. 2 L. 580/93, i servizi specifici che le Camere di commercio sono tenute a fornire sull’intero territorio nazionale, in relazione alle funzioni amministrative ed economiche di cui alla suddetta norma, sono state definite dal D.M. 7 marzo 2019.

1.2 Panoramica del trattamento

1.2.1 Quale è il trattamento in considerazione?

Il trattamento oggetto della presente “DPIA” (Data Privacy Impact Assessment) concerne l'acquisizione e la gestione delle segnalazioni di illeciti “c.d. whistleblowing”, così come disciplinate dal D.lgs. n. 24 del 2023 che ha recepito la Direttiva UE n. 1937/2019.
La metodologia di analisi adottata segue la struttura della piattaforma rilasciata dal Garante Privacy Francese (CNIL) e risponde a tutti i criteri indicati dalla normativa di riferimento.

1.2.2 Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento dei dati: è la Camera di Commercio, Industria, Agricoltura e Artigianato di Cuneo

Responsabile del trattamento: Whistleblowing Solution Srl con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961.

1.2.3 Ci sono standard applicabili al trattamento?

D. L.gs. n. 24 del 2023
Direttiva UE n. 1937/2019
Linee Guida ANAC del 12 luglio 2023
Regolamento UE n. 2016/679 (c.d. GDPR)
D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018

1.3 Dati, processi e risorse di supporto

1.3.1 Tipologia di dati raccolti

Dati comuni: I dati trattati sono quelli inseriti nella segnalazione e, se del caso, acquisiti nel corso delle istruttorie. Tali dati comprendono dati comuni (tra cui l'identità del segnalante, del segnalato, i ruoli dagli stessi ricoperti). Inoltre, il segnalante può avvalersi anche della segnalazione orale mediante invio di una mail all’indirizzo anticorruzione@cn.camcom.it.

Dati particolari e relativi a condanne penali e reati: L'acquisizione e la gestione delle segnalazioni potrebbe dar luogo a trattamenti di dati personali, anche appartenenti a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti dai segnalanti.

1.3.2 Categorie di interessati

Segnalanti (Dipendenti, Liberi professionisti e consulenti che prestano la propria attività presso l'Ente stagisti, tirocinanti, retribuiti e non retribuiti, Componenti degli organi di gestione e controllo).

1.3.3 Soggetti (interni) che possono accedere ai dati

La piattaforma WEB consente l'accesso alle segnalazioni e alla documentazione allegata unicamente al RPCT e al gruppo di lavoro / dipendenti camerali che supporta/no RPCT, previa assegnazione da parte di quest'ultimo della segnalazione stessa.

1.3.4 Comunicazione e/o diffusione dei dati

I trattamenti analizzati con la presente DPIA non comportano comunicazione né diffusione dei dati.
Sono fatte salve specifiche e puntuali comunicazioni della segnalazione, in conformità alla legge, all'Autorità Giudiziaria, Corte dei Conti e/o l'A.N.A.C, che opereranno ciascuno nell'ambito delle rispettive competenze, in qualità di Titolari autonomi del trattamento.
I dati personali raccolti con la segnalazione, inoltre, potranno essere comunicati ai soggetti segnalati, solo in caso di consenso espresso del segnalante e nelle ipotesi previste dal D. Lgs. n. 24/2023.
In particolare, nell'ambito dei procedimenti disciplinari, l'identità del segnalante potrà essere rivelata laddove concorrano, insieme, i seguenti tre presupposti:

- che la contestazione si fondi, in tutto o in parte, sulla segnalazione;
- che la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato;
- che il segnalante abbia espresso un apposito consenso alla rivelazione della propria identità.

1.3.5 Descrizione del "ciclo di vita" del trattamento

I Dati vengono conservati e mantenuti nella Piattaforma per il tempo strettamente necessario al conseguimento delle finalità previste, e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. Parimenti, nel caso in cui la segnalazione avvenga nel corso di un colloquio in presenza del RPCT, i dati verranno trattati nelle stesse modalità e mantenuti per il tempo strettamente necessario al conseguimento delle finalità previste e, comunque, non oltre anni cinque dalla data della comunicazione dell'esito finale della procedura in oggetto.
Nel caso di contenzioso o di segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrà essere protratto anche oltre i termini sopra indicati, fino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

1.3.6 Sistemi operativi, server, software, reti e altri supporti che ospitano i dati.

La Camera di commercio si avvale, per la gestione delle segnalazioni, di una piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.

L'infrastruttura applicativa è una piattaforma esclusivamente dedicata, sviluppata per soddisfare le esigenze in fatto di sicurezza e riservatezza, punto essenziale della procedura di whistleblowing. La gestione degli accessi e dei dati avviene nel più rigoroso rispetto del quadro normativo ed è certificata dai più rigorosi standard ovvero:

- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID
- Certificazione CSA Star

La piattaforma web Segnalazione Illeciti - Whistleblowing si suddivide in un Portale pubblico / Ambiente di Segnalazione dedicato ai segnalanti e un Pannello gestionale / Area di Amministrazione dedicato al Responsabile della segnalazione (o ai Responsabili e ad eventuali Collaboratori incaricati).

La gestione delle segnalazioni non avviene tramite altri canali. Infatti, anche nell'ipotesi in cui il segnalante chieda un appuntamento a RPCT, quest'ultimo provvederà a inserire la segnalazione raccolta oralmente direttamente nella piattaforma.

Tutte le attività istruttorie, avviate in seguito alla segnalazione, sono gestite nell'ambito della piattaforma, così come le comunicazioni con il segnalante, il segnalato ed eventuali ulteriori soggetti (informatori).

2 Principi Fondamentali

2.1 Proporzionalità e necessità

2.1.1 Specificità e legittimità degli scopi perseguiti

I dati trattati dalla Camera di commercio nell'ambito delle procedure c.d. whistleblowing sono trattati esclusivamente per ricevere e gestire le segnalazioni di violazioni presentate ai sensi del D. Lgs. 10 marzo 2023, n. 24, effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e procedere all'adozione di tutti i conseguenti provvedimenti.
I dati non sono trattati per ulteriori finalità.

2.1.2 Basi giuridiche del trattamento

Il trattamento di dati comuni (dati identificativi e di contatto del segnalante, dell'autore delle violazioni o di altre persone a vario titolo coinvolte nelle vicende segnalate) costituisce l'adempimento di un obbligo legale e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR.
Nel caso in cui vengano trattati dati appartenenti a categorie particolari, la base giuridica è rappresentata dall'art. 9.2, lett. b) e g) GDPR, in connessione con l'art. 2-sexies, comma 2, lett. dd), del D.Lgs. n.196/2003.
Per i dati personali relativi a condanne penali e misure di sicurezza, la base giuridica è rappresentata dall'art. 2-octies, comma 3, lett. a), del D.Lgs. n. 196/2003.
I dati personali sono trattati sulla base del consenso espresso del segnalante ai fini della conoscibilità della segnalazione ove la stessa sia necessaria alla difesa dell'incolpato, anche nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023).

2.1.3 Minimizzazione dei dati (adeguatezza, pertinenza, limitatezza)

I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).
L'identità del segnalante è separata dalla segnalazione ed è conoscibile a RPCT solo ove ciò sia funzionale alla corretta gestione della segnalazione.

2.1.4 Esattezza e aggiornamento dei dati

Nel caso di segnalazioni palesemente infondate le stesse vengono immediatamente archiviate. Nel caso di informazioni non coerenti, nell'ambito dell'istruttoria RPCT e i soggetti autorizzati alla gestione della segnalazione possono aggiornare i dati, chiedere eventuali integrazioni o rettifiche che sono comunque inserite nel fascicolo della segnalazione. Inoltre, il segnalante può sempre interloquire con RPCT, tramite la piattaforma, al fine di chiedere la modifica / integrazione delle informazioni trasmesse.

2.1.5 Periodo di conservazione dei dati

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, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

Nel caso di contenzioso o di segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrà essere protratto anche oltre i termini sopra indicati, fino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

2.2 Misure a tutela dei diritti degli Interessati

2.2.1 Modalità di rilascio dell'informativa in materia di protezione dei dati

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità:

- Comunicazione a tutti i dipendenti sull'esistenza del canale di segnalazione interno;
- Pubblicazione sito web istituzionale – sezione dedicata al Whistleblowing (https://www.cn.camcom.it/amministrazione-trasparente/altri-contenuti/prevenzione-della-corruzione/segnalazione-condotte).

2.2.2 Conferimento, conservazione e revoca del consenso al trattamento dei dati

Il trattamento dei dati personali acquisiti con la segnalazione e nell'ambito delle successive attività istruttorie non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR.

Il consenso degli interessati costituisce la base giuridica unicamente per la comunicazione dell'identità del segnalante al segnalato, ove la stessa sia necessaria alla difesa dell'incolpato nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023). La piattaforma consente di raccogliere il consenso del segnalante per tale fine al momento dell'invio della segnalazione, tramite apposito form.

2.2.3 Esercizio del diritto di accesso

Quanto al diritto di accesso, si segnala che tale diritto non appare immediatamente esercitabile poiché limitato ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "*1. 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 (...) f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58*".

L'interessato può comunque avanzare la richiesta ai dati di contatto indicati dal Titolare del trattamento nell'informativa fornita ai sensi degli artt. 13 e 14 oppure contattando direttamente il Data Protection Officer nominato dall'Ente.
La Camera di commercio effettuerà tutte le valutazioni del caso, tenendo sempre in considerazione l'obbligo di garantire la riservatezza del segnalante.

2.2.4 Esercizio del diritto di portabilità

Le operazioni di trattamento oggetto della presente DPIA trovano fondamento nell' adempimento di obbligo di legge e nell'esecuzione di un compito di interesse pubblico, ai sensi degli artt. 6, par. 1, lett. c) ed e) e 9 par. 2, lett. g) del GDPR: pertanto il diritto alla portabilità non è applicabile.
Infatti, ai sensi dell'art. 20 GDPR, tale diritto può essere esercitato quando ricorrono congiuntamente i due seguenti presupposti:

- il trattamento si basi sul consenso ai sensi dell'articolo 6, paragrafo 1, lettera a), o dell'articolo 9, paragrafo 2, lettera a), o su un contratto ai sensi dell'articolo 6, paragrafo 1, lettera b) e;
- il trattamento sia effettuato con mezzi automatizzati".

2.2.5 Esercizio del diritto di rettifica

Quanto al diritto di rettifica, il segnalante può sempre accedere alla piattaforma al fine di segnalare con ulteriori e successive comunicazioni eventuali dati inesatti.
Le ulteriori richieste di rettifica sono valutate alla luce della previsione di cui all'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. 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 (...) f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58.

2.2.6 Esercizio del diritto di cancellazione

Il diritto alla cancellazione non è applicabile al caso di specie, ai sensi dell'art. 17, par. 3, GDPR a norma del quale: "*I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: (…) b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse*".

2.2.7 Esercizio del diritto di limitazione

Il diritto alla limitazione non appare esercitabile, ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: *"1. 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 (...) f) alla riservatezza dell'identita' della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58.*

2.2.8 Esercizio del diritto di opposizione

Non è previsto il riconoscimento del diritto di opposizione, sussistendo motivi legittimi cogenti per procedere al trattamento, in considerazione delle finalità di interesse pubblico perseguite, degli interessi connessi al buon andamento della PA, nonché della necessità e proporzionalità del trattamento medesimo.

2.2.9 Definizione e contrattualizzazione degli obblighi posti in capo al Responsabile del trattamento

Whistleblowing PA Srl è stata formalmente nominata quale Responsabile del trattamento (All. 2).
La Nomina risponde ai criteri di cui all'art. 28 GDPR.

2.2.10 Trasferimento dei dati al di fuori dello Spazio Economico Europeo

I dati non sono trasferiti al di fuori dei Paesi dell'Unione Europea.
Whistleblowing PA srl dichiara nelle specifiche tecniche e nella Nomina che i server che supportano il software segnalazioni.net sono ubicati in Italia

3 Rischi

3.1 Misure di sicurezza

In questa sottosezione vengono elencate e descritte le misure di sicurezza di carattere tecnico od organizzativo, che contribuiscono alla sicurezza dei dati trattati.

Si rimanda, per esigenze di completezza, al punto 4 della Documentazione a supporto del Titolare per la valutazione di impatto sulla protezione dei dati (All. 1). Le misure adottate dal gestore della piattaforma, Whistleblowing Solutions S.r.l., sono le seguenti:

Misura di sicurezza
Backup
Contrasto al malware e agli attacchi informatici
Contratto con il Responsabile del trattamento
Controllo accesi logici
Controllo accessi fisici
Crittografia
Gestione del personale
Manutenzione
Minimizzazione dei dati
Politica di tutela della privacy
Protezione contro fonti di rischio non umane
Sicurezza dei canali informatici
Tracciabilità (log)
Vulnerabilità
Gestire gli incidenti di sicurezza e la violazione dei dati personali
Disaster recovery
Business continuity

3.2 Profilo della Riservatezza: accesso illegittimo ai dati

3.2.1 Principali impatti/danni che potrebbero subire gli Interessati

- Condotte ritorsive (il licenziamento, la sospensione o misure equivalenti, la retrocessione di grado o la mancata promozione, il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria, la coercizione, l'intimidazione, le molestie o l'ostracismo, la discriminazione o comunque il trattamento sfavorevole, la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione, il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e

la perdita di redditi, l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro, la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso, la richiesta di sottoposizione ad accertamenti psichiatrici o medici).

- Conseguenze di carattere reputazionale
- Difficoltà nelle relazioni lavorative e sociali
- Aumento stress lavorativo
- Estorsione (anche sotto forme di tentativo)

3.2.2 Principali minacce che potrebbero concretizzare il rischio

- Negligente custodia delle credenziali di accesso alla Piattaforma
- Utilizzo improprio / cessioni di credenziali per l'accesso alla Piattaforma
- Intercettazioni delle trasmissione o dei dati
- Data Breach subito dal Responsabili del trattamento
- L'identità del segnalante rivelata a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni
- Violazione delle piattaforma da parte di attaccanti esterni

3.2.3 Fonti di rischio (umane e non umane)

- Fonti umane interne (RPCT, dipendenti, collaboratori)
- Fonti umane esterne (Fornitori, attaccanti).

3.2.4 Misure di sicurezza che contribuiscono a mitigare il rischio

- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Crittografia
- Tracciabilità
- Controllo degli accessi logici
- Contratto con il responsabile del trattamento
- Lotta contro il malware
- Vulnerabilità
- Sicurezza dei canali informatici
- Manutenzione
- Controllo degli accessi fisici
- Politica di tutela della privacy
- Gestione delle risorse umane

3.2.5 Stima della gravità del rischio

(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☐	☐	☒	☐

Motivazione:

La gravità del rischio è valutata Importante in considerazione delle categorie dei soggetti interessati (soggetti segnalanti oggetto di possibili condotte ritorsive, ma anche soggetti segnalati passibili di procedimenti disciplinari o giudiziari a loro carico), nonché delle possibili conseguenze a carico degli stessi in caso di violazione della riservatezza.

3.2.6 Stima della probabilità del rischio

(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☐	☒	☐	☐

Motivazione:

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte e come rappresentate nell'All. 1) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy.

In particolare, le misure di sicurezza approntate proteggono la riservatezza dell'identità sia del whistleblower, sia della persona segnalata, sia di qualsiasi altra persona comunque menzionata nella segnalazione, nonché la riservatezza del contenuto della segnalazione e della relativa documentazione. Ciò è garantito anche tramite il ricorso a strumenti di crittografia.

3.3 Profilo dell'Integrità: modifiche indesiderate dei dati

3.3.1 Principali impatti/danni che potrebbero subire gli Interessati

- Ingiusto coinvolgimento del segnalato in procedimenti disciplinari e/o giudiziari;
- Condotte ritorsive (il licenziamento, la sospensione o misure equivalenti; la retrocessione di grado o la mancata promozione; il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro; la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa; le note di merito negative o le referenze negative; l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria; la coercizione, l'intimidazione, le molestie o l'ostracismo; la discriminazione o comunque il trattamento sfavorevole; la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione; il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi; l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel

settore o nell'industria in futuro; la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso; la richiesta di sottoposizione ad accertamenti psichiatrici o medici);

- Estorsione (anche sotto forme di tentativo).

3.3.2 Principali minacce che potrebbero concretizzare il rischio

- Negligente custodia delle credenziali di accesso alla Piattaforma;
- Utilizzo improprio / cessioni di credenziali per l'accesso alla Piattaforma;
- Intercettazioni delle trasmissione o dei dati;
- Data Breach subito dal Responsabili del trattamento;
- Violazione delle piattaforma da parte di attaccanti esterni.

3.3.3 Fonti di rischio (umane e non umane)

- Fonti umane interne (RPCT, dipendenti, collaboratori);
- Fonti umane esterne (Fornitori, attaccanti).

3.3.4 Misure di sicurezza che contribuiscono a mitigare il rischio

- Gestire gli incidenti di sicurezza e le violazioni dei dati personali;
- Crittografia;
- Tracciabilità;
- Controllo degli accessi logici;
- Contratto con il responsabile del trattamento;
- Lotta contro il malware;
- Backup;
- Disaster recovery;
- Business continuity;
- Vulnerabilità;
- Sicurezza dei canali informatici;
- Manutenzione;
- Controllo degli accessi fisici;
- Protezione contro fonti di rischio non umane;
- Politica di tutela della privacy;
- Minimizzazione del trattamento;
- Gestione del personale.

3.3.5 Stima della gravità del rischio

(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☐	☐	☒	☐

Motivazione:

La gravità del rischio è valutata Importante in considerazione delle categorie dei soggetti interessati (soggetti segnalanti oggetto di possibili condotte ritorsive, ma anche soggetti segnalati passibili di procedimenti disciplinari o giudiziari a loro carico), nonché delle possibili conseguenze a carico degli stessi in caso di violazione dell'integrità dei dati.

3.3.6 Stima della probabilità del rischio

(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☐	☒	☐	☐

Motivazione:

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy.

3.4 Profilo della Disponibilità: perdita di dati

3.4.1 Principali impatti/danni che potrebbero subire gli Interessati

- Mancata definizione dell'istruttoria e conseguenti possibili problematiche di natura giuslavoristica e contrattuale.

3.4.2 Principali minacce che potrebbero concretizzare il rischio

- Fonti umane interne (RPCT, dipendenti, collaboratori);
- Fonti umane esterne (Fornitori, attaccanti);
- Fonti non umane (incendi, terremoti, inondazioni, ecc.);

3.4.3 Fonti di rischio (umane e non umane)

- Fonti umane interne (RPCT, dipendenti, collaboratori);
- Fonti umane esterne (Fornitori, attaccanti);
- Fonti non umane (incendi, terremoti, inondazioni, ecc.).

3.4.4 Misure di sicurezza che contribuiscono a mitigare il rischio

- Gestire gli incidenti di sicurezza e le violazioni dei dati personali;
- Contratto con il responsabile del trattamento;
- Backup;
- Disaster recovery;
- Business continuity;
- Vulnerabilità;

- Sicurezza dei canali informatici;
- Manutenzione;
- Controllo degli accessi fisici;
- Protezione contro fonti di rischio non umane;
- Politica di tutela della privacy.

3.4.5 [Perdita] Stima della gravità del rischio

(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☐	☒	☐	☐

Motivazione:

Le modifiche indesiderate dei dati potrebbero comportare ricadute nell'iter amministrativo dei processi dell'Ente, comportando possibili ricadute di natura contrattuale rispetto agli interessati. Tali difficoltà risutlano comunque superabili anche se con *effort* di tempo e di risorse dedicate alle necessarie rettifiche / integrazioni.

3.4.6 Stima della probabilità del rischio

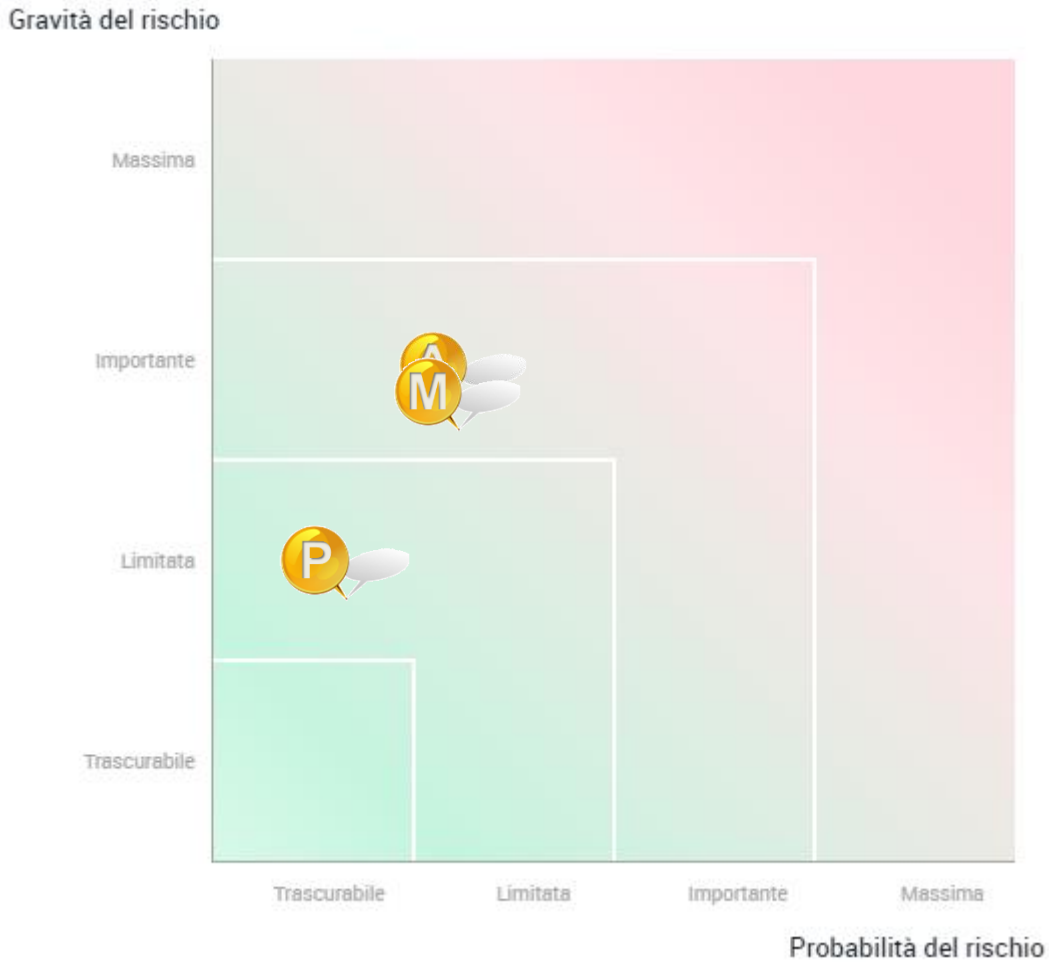
(Indefinito)	*Trascurabile*	*Limitato*	*Importante*	*Massimo*
☐	☒	☐	☐	☐

Motivazione:

Le politiche di disaster recovery, il sistema di business continuity e di vulnerability, nonchè i sistemi di backup adottati dal Responsabile del trattamento riducono la gravità del rischio.

4. Mappatura complessiva del rischio

La seguente rappresentazione grafica consente di confrontare il posizionamento del rischio prima e dopo l'applicazione delle misure aggiuntive.



Legenda:	
Rischio attuale: A *Accesso ai dati* M *Modifica dei dati* P *Perdita di dati*	

5. Parere del DPO ed eventuale consultazione degli Interessati

La presente sezione riporta il parere sulla DPIA reso dal DPO, nonché le valutazioni circa la necessità o meno di effettuare una previa consultazione dei soggetti Interessati o potenziali tali. Ove tale consultazione è stata effettuata, nella sezione vengono riportati i relativi risultati.

5.1 Parere reso dal DPO e Accountability del Titolare

Ai sensi e per gli effetti del combinato disposto degli artt. 35, par. 2 e 39, par. 1, lett. *c)* del GDPR, a seguito della redazione dei precedenti paragrafi gli stessi sono stati trasmessi all' Ing. Maria Paola Manconi, Responsabile della protezione dei dati personali (DPO) dell'Ente il quale in data 14.5.2024 ha formulato il parere di seguito riportato, secondo cui, in sintesi:

☒ il trattamento può essere avviato / continuato

☐ il trattamento non dovrebbe essere avviato / continuato

In relazione a tale parere, tenuto conto del par. 4.2 delle Linee guida WP243:

X il Titolare del trattamento concorda con le indicazioni fornite dal DPO

☐ il Titolare non concorda con le indicazioni fornite dal DPO (per le ragioni di seguito esposte)

5.2 Consultazione degli Interessati o dei loro rappresentanti

Tenuto conto dell'art. 35, par. 9 del GDPR, ai sensi del quale il Titolare del trattamento, ove opportuno, "*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*":

☐ il Titolare del trattamento ha ritenuto opportuno coinvolgere gli Interessati o i loro rappresentanti	
Modalità di coinvolgimento:	
Esito:	
☒ il Titolare del trattamento ha deciso di **non** raccogliere le opinioni degli Interessati	
Motivazioni del mancato coinvolgimento:	Il Titolare, trattandosi di adempimenti connessi a obblighi di legge che trovano dettagliata disciplina nella vigente normative e in specifiche Linee Guida ANAC; non ha ritenuto necessario chiedere il parere degli interessati, che peraltro appartengono a svariate categorie non sempre rappresentate. Tuttavia, come previsto dalla normativa, il Titolare ha informato le rappresentanze sindacali dell'adozione della Piattaforma e delle procedure di segnalazione.