Provincia *di* Ancona

Provincia *di* Ancona

DECRETO DEL PRESIDENTE DELLA PROVINCIA

N. 41 DEL 10/04/2025

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

L'anno 2025 il giorno 10 del mese di aprile alle ore 17:14, nella sede della Provincia, convocata nei modi di legge, si è tenuta la seduta presidenziale: il Presidente, CARNEVALI DANIELE, con la partecipazione del Segretario Generale, SAVINI MARINA, ai sensi dell'art. 97 del D.Lgs. n. 267/2000 e s.m.i. e dell'art.37, comma 6, dello Statuto della Provincia di Ancona.

ADOTTA

il decreto di seguito riportato.

.

Provincia di Ancona

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

IL PRESIDENTE

VISTO lo Statuto della Provincia di Ancona (adeguato alla legge 7 aprile 2014, n. 56) adottato dall'Assemblea dei Sindaci con deliberazione n. 3 del 02/02/2015 e modificato con gli atti n. 2 del 28/04/2017, n. 4 del 20/12/2022 e, da ultimo, n. 2 del 16/01/2024;

VISTI:

- la Legge 6 novembre 2012, n. 190, recante "*Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella Pubblica Amministrazione*", che, all'art. 1, comma 51, aveva modificato il D. Lgs. n. 165 del 2001, inserendovi l'articolo 54-bis, in virtù del quale era stato introdotto nell'ordinamento italiano l'istituto del whistleblower, finalizzato a favorire l'emersione delle fattispecie di illecito all'interno delle Pubbliche Amministrazioni
- la Legge 30 novembre 2017, n. 179 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato";
- la 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 (istituto del whistelblowing);
- il D. Lgs. 10 marzo 2023, n. 24, 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 e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.";
- le Linee Guida dell'Autorità Nazionale Anticorruzione (A.N.A.C.) in materia di whistleblowing approvate con Deliberazione n. 311 del 12 luglio 2023;

RICHIAMATO il decreto del Presidente della Provincia di Ancona n. 137 del 19/10/2023 avente ad oggetto "Procedura di segnalazione di violazioni di disposizioni normative nazionali o dell'Unione Europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica (cd Whistleblowing) - Adeguamento disciplina della tutela della persona che segnala violazioni (D.lgs. n. 24/2023 e Linee guida deliberazione A.N.AC. n. 311/2023);

DATO ATTO che con il suddetto decreto n.137/2023 era stato aggiornato anche il format online di segnalazione d'illeciti da parte del dipendente pubblico c.d. *whistleblower;*

RITENUTO NECESSARIO provvedere all'adeguamento della citata procedura di gestione mediante l'approvazione di una nuova procedura che sostituisce integralmente la precedente;

RICHIAMATO in particolare l'art. 4, comma 1, del citato D.lgs. n. 24/2023, il quale stabilisce che "I soggetti del settore pubblico […], sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano, ai sensi del presente articolo, 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. […]";

CONSIDERATO altresì che l'art. 4, comma 5, del citato D. Lgs. n. 24/2023 prevede: "I soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna.";

DATO ATTO che con decreto del Presidente della Provincia di Ancona n. 62 del 03/05/2022 è provveduto alla nomina del Responsabile della prevenzione della corruzione e della trasparenza (RPCT), prevedendo il ruolo in capo al Segretario Generale, Dott.ssa Marina Savini;

PRESO ATTO che:

- il Piano Nazionale Anticorruzione (PNA) 2022, approvato con delibera n. 7 del 17 gennaio 2023 dall'Autorità Nazionale Anticorruzione, riconduce espressamente la tutela del dipendente che segnala condotte illecite tra le azioni e le misure generali finalizzate alla prevenzione della corruzione, in particolare fra quelle obbligatorie;
- il sistema di prevenzione della corruzione, introdotto dalla legge n.190/2012 deve realizzarsi attraverso un'azione coordinata tra un livello nazionale ed uno "decentrato";
- il PNA impone alle pubbliche amministrazioni, di cui all'art. 1, comma 2, del D.lgs. n.165/2001, l'assunzione dei "*necessari accorgimenti tecnici per dare attuazione alla tutela del dipendente che effettua le segnalazioni*".;
- le Linee Guida ANAC Delibera n. 311 del 12/07/2023- danno indicazioni affinché il canale di segnalazione interna debba garantire la riservatezza, anche tramite il ricorso a strumenti di crittografia, ove siano utilizzati strumenti informatici dei seguenti elementi:
  a) della persona segnalante;
  b) del facilitatore;
  c) della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
  d) del contenuto della segnalazione e della relativa documentazione.

RITENUTO NECESSARIO, per le ragioni sinora esposte, approvare una nuova procedura informatizzata, al fine di disciplinare la gestione delle segnalazioni "whistleblowing" effettuate dai dipendenti dell'ente e dagli altri soggetti legittimati, in ottemperanza alla nuova disciplina introdotta dal decreto legislativo 10 marzo 2023, n. 24 (attuativo della Direttiva europea 1937/2019);

VISTO il software opensource WhistleblowingIT proposto gratuitamente per le Pubbliche

Amministrazioni da Whistleblowing Solution Impresa Sociale, in collaborazione con Transparency International Italia all'interno di un progetto, sostenuto anche dall'Internal Security Fund dell'Unione Europea, nato per offrire a tutte le Pubbliche Amministrazioni un software informatico gratuito per dialogare con i segnalanti, grazie a modalità che garantiscono l'anonimato;

RILEVATO che il citato software (SW) WhistleblowingIT:

a) è basato sul software GlobaLeaks, che permette al Responsabile per la Prevenzione della Corruzione di ricevere le segnalazioni di illeciti da parte di tutti i soggetti previsti dalla normativa, anche in modo anonimo;
b) è disponibile con un questionario appositamente studiato da Transparency International Italia per il contrasto degli illeciti ed è progettata in conformità al decreto legislativo n. 24/2023
c) Il servizio di whistleblowing digitale offerto nell'ambito di questo progetto ha ottenuto la qualificazione dall'Agenzia per la Cybersicurezza Nazionale (ACN).
d) possiede le certificazioni di qualità ISO 9001:2015, ISO 27001:2022 e CSA Star Level 1;
e) è conforme al principio DNSH;

VISTO il contratto di servizio (Allegato 1) e la documentazione tecnica predisposti da Whistleblowing Solution, nonché l'accordo in merito al trattamento dei dati personali ai fini della nomina a Responsabile del trattamento ai sensi del GDPR (Allegato 2);

CONSIDERATO che ai fini dell'adozione di una procedura aggiornata, e considerata la volontà di adesione al progetto WhistleblowingIT per la gestione delle segnalazioni con piattaforma informatica, è necessario provvedere alla stesura di una dettagliata valutazione di impatto DPIA ai sensi dell'art. 35 REGOLAMENTO (UE) 2016/679 (GDPR);

VISTA la DPIA predisposta dal Responsabile della protezione dei dati (DPO) della Provincia di Ancona prot. n. del (Allegato 3);

DATO ATTO che ai sensi dell'art. 13 del D.lgs. n. 24/2023 il nuovo format online di segnalazione è stato oggetto di informativa alla RSU e Organizzazioni Sindacali in data 02/04/2025 (prot. 12408/2025);

VISTA l'informativa "Segnalazione Condotte Illecite" ai sensi degli articoli 13 -14 del Regolamento (UE) n. 2016/679 "GDPR; (Allegato 4);

RITENUTO pertanto opportuno:

- aggiornare la procedura di gestione delle segnalazioni ai sensi del D.lgs. n. 24/2023;
- prevedere nella procedura l'istituzione di apposito canale di segnalazione interno;
- consentire al segnalante la scelta, nel canale interno tra l'utilizzo di una piattaforma informatica dedicata ovvero la segnalazione in forma orale al gestore delle segnalazioni;
- individuare nel gestore delle segnalazioni whistleblowing, il RPCT, e contestualmente autorizzarlo al trattamento dei dati connessi;
- aderire al progetto WhistleblowingIT di Whistleblowing Solution e Transparency International Italia per la piattaforma informatica di segnalazione;

DATO ATTO che ai fini dell'adozione del presente provvedimento non sussiste conflitto di

interessi di cui all'art. 6-bis della Legge n. 241/1990, come introdotto dalla Legge n. 190/2012, da parte del Responsabile del procedimento e Dirigente responsabile;

PRESO ATTO che sulla proposta non necessita acquisire il parere di regolarità contabile, non rivestendo la stessa alcun aspetto che direttamente o indirettamente presenti profili finanziari, economici o contabili;

DECRETA

1. di aderire, per l'attivazione della piattaforma informatica di segnalazione di gestione delle segnalazioni di illecito a norma del D.lgs. 10 marzo 2023, n. 24, che recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, la quale sostituisce integralmente le precedenti procedure in uso all'Ente, al progetto WhistleblowingIT, con software opensource proposto gratuitamente per le Pubbliche Amministrazioni da Whistleblowing Solution Impresa Sociale in collaborazione con Transparency International Italia;
2. di approvare lo schema di contratto di servizio proposto da Whistleblowing Solution Impresa sociale, in allegato al presente atto per formarne parte integrante e sostanziale (All.1 Contratto di servizio WBPA);
3. di individuare il soggetto gestore delle segnalazioni whistleblowing nel RPCT, Segretario generale (Allegato 2);
4. di demandare all'RPCT, nonché Segretario Generale, le ulteriori attività necessarie a dare attuazione al presente atto;
5. di pubblicare il presente decreto all'Albo Pretorio online per 15 giorni consecutivi, ai sensi del combinato disposto degli artt. 124, comma 1, e 134, comma 3, del T.U.E.L.;
6. di pubblicare altresì il presente decreto nella sezione "Amministrazione Trasparente" del sito istituzionale dell'Ente www.provincia.ancona.it, ai sensi dell'art. 12 del D.lgs. n. 33/2013 e nella sezione "Altri contenuti ◊ Prevenzione della corruzione";
7. di dare esecuzione al procedimento con il presente disposto designandone, a norma dell'art. 5 della legge 241/1990, a responsabile la Dott.ssa Laura Lampa, Responsabile dell'Area Affari Generali;
8. di dichiarare il presente decreto immediatamente eseguibile ai sensi dell'art. 134, comma 4, del T.U.E.L., per procedere all'adozione della procedura in oggetto.

Provincia di Ancona

PARERE DI REGOLARITA' TECNICA

(di cui all'art. 49 T.U. D.lgs. 18.8.2000, n. 267 e s.m.i.)

PROPOSTA DI DECRETO

N. 1086/2025

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

Si esprime parere FAVOREVOLE sulla proposta di decreto indicata in oggetto in ordine alla regolarità tecnica.

Ancona, 10/04/2025

IL DIRIGENTE DEL SETTORE

BASSO FABRIZIO

(sottoscritto digitalmente ai sensi dell'art. 21 D.lgs. n. 82/2005 e s.m.i.)

Provincia di Ancona

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.Lgs. n. 82/2005 e s.m.i.

IL SEGRETARIO GENERALE
SAVINI MARINA

IL PRESIDENTE DELLA PROVINCIA
CARNEVALI DANIELE

Classificazione 01.01.02
Fascicolo 2018/33

.

CONTRATTO DI SERVIZIO

Documento aggiornato il 20 settembre 2023

Il seguente contratto regola il rapporto di fornitura e fruizione dei servizi offerti sul sito www.whistleblowing.it.

1. DEFINIZIONI

1.1. CONTRATTO: indica il presente Contratto di Servizio;

ENTE: indica il soggetto che accetta il seguente CONTRATTO al fine di utilizzare i SERVIZI predisposti dal FORNITORE;

FORNITORE: Whistleblowing Solutions Impresa Sociale S.r.l.;

PIATTAFORMA: indica la piattaforma di whistleblowing digitale personale dell'ENTE;

SERVIZI: predisposizione e fornitura di risorse informatiche e materiale per la formazione da parte del FORNITORE a beneficio dell'ENTE, al fine di usufruire di un servizio di Whistleblowing Digitale basato su software GlobaLeaks ed erogato in modalità Software as a Service (SaaS).

2. OGGETTO DEL CONTRATTO

2.1 Premesso che GlobaLeaks è un software open-source creato per permettere l'avvio di iniziative di whistleblowing sicuro ed anonimo rilasciato sotto licenza AGPL (Affero General Public License), che l'utilizzo di software open-source riveste un'importanza fondamentale per il FORNITORE, e che la licenza open-source potrebbe includere disposizioni che prevalgono espressamente su alcuni dei presenti termini.

2.2 Il FORNITORE propone all'ENTE la stipula delle condizioni che consentono allo stesso di usufruire dei seguenti SERVIZI in modalità completamente gratuita:

a. accesso ad una PIATTAFORMA di whistleblowing digitale basata sul software GlobaLeaks che permette di ricevere segnalazioni di illeciti da parte dei potenziali segnalanti e di dialogare con gli stessi, anche in modo anonimo;
b. possibilità di esportazione dati e configurazioni per migrazione su sistemi informativi autonomi garantita dall'utilizzo di una tecnologia open-source (no lock-in);
c. materiali formativi in modalità e-learning;
d. invio di materiale informativo in relazione ad aggiornamenti tecnici e normativi in materia di whistleblowing;

e. testi specifici sul whistleblowing e sull'utilizzo della piattaforma da pubblicare sul sito dell'ENTE;
f. modelli di materiali di comunicazione a scopo informativo e di sensibilizzazione dei potenziali segnalanti.

2.3 Le personalizzazioni sono limitate all'inserimento del logo dell'ENTE e al caricamento di testi personalizzati nella homepage della PIATTAFORMA.

3. ACCESSO AI SERVIZI

3.1 L'accesso ai SERVIZI è consentito a seguito della registrazione sul sito www.whistleblowing.it. Completata la registrazione, l'ENTE ha accesso alla PIATTAFORMA offerta in modalità SaaS e accessibile tramite internet. Il FORNITORE avrà il diritto di modificare le modalità di accesso e di utilizzo dei SERVIZI, anche in ragione del mutamento delle tecnologie telematiche nonché in ragione della variazione delle caratteristiche tecniche dei software applicativi e di base (sistemi operativi e infrastrutture tecnologiche).

3.2 Con la registrazione, l'ENTE assicura che tutti i dati personali e aziendali da lui trasmessi nell'ambito della registrazione stessa e dell'account creato siano completi e corretti in termini di contenuto.

4. UTILIZZO DEI SERVIZI

4.1 L'ENTE è responsabile del corretto utilizzo della PIATTAFORMA e il FORNITORE non è responsabile né dell'uso improprio della stessa né della perdita delle credenziali di accesso.

4.2 I dati contenuti negli archivi della propria PIATTAFORMA sono di esclusiva proprietà dell'ENTE e possono essere trattati direttamente solo dallo stesso. I dati potranno essere inseriti, variati, elaborati, o comunque trattati, solo ed esclusivamente nei modi e nelle forme previste dai SERVIZI messi a disposizione dal FORNITORE.

4.3 Considerate le misure crittografiche sicure implementate le parti convengono che la conservazione delle chiavi crittografiche avvenga secondo l'Opzione A descritta nel documento Modalità di Conservazione delle Chiavi Crittografiche allegato al presente CONTRATTO.

4.4 L'ENTE è tenuto a comunicare tempestivamente al FORNITORE qualsiasi abuso di cui venga a conoscenza.

4.5 L'ENTE non è autorizzato a utilizzare la PIATTAFORMA in qualsiasi modo incompatibile con il presente CONTRATTO o qualsiasi normativa applicabile. In particolare, l'ENTE o il personale autorizzato ad utilizzare la PIATTAFORMA non potranno:

a. utilizzare la PIATTAFORMA e i SERVIZI per finalità illecite o non autorizzate;
b. duplicare, trasferire, autorizzare, assegnare, dare accesso a o copiare la PIATTAFORMA, senza la previa autorizzazione scritta del FORNITORE;

c. tentare di modificare, adattare o alterare alcuna parte della PIATTAFORMA o dei SERVIZI;
d. interferire con o interrompere il funzionamento della PIATTAFORMA o dei SERVIZI, dei server o delle reti a questo collegati, ivi compreso attraverso l'utilizzo e/o la trasmissione di worm, virus, spyware, malware o qualsiasi altro codice che presenti una natura distruttiva o perturbatrice;
e. introdurre contenuti o codici o interferire in qualsiasi altra maniera con le modalità attraverso le quali la PIATTAFORMA è resa disponibile o mostrata sul browser;
f. richiedere i SERVIZI attraverso mezzi o modalità non autorizzati, incluso, a titolo esemplificativo e non esaustivo, attraverso l'utilizzo di dispositivi automatizzati, script, bot, spider, crawler o scraper;
g. eludere, rimuovere, spegnere o disattivare in altro modo le misure di sicurezza implementate.

4.6 L'ENTE è tenuto ad utilizzare l'ultima versione disponibile dei SERVIZI e della PIATTAFORMA come aggiornata per miglioria evolutiva o di sicurezza dal FORNITORE.

4.7 L'ENTE deve creare autonomamente e sotto la propria responsabilità e a proprie spese tutte le condizioni necessarie per l'utilizzo dei SERVIZI. Ciò vale in particolare per i terminali remoti che dovranno essere adeguati e compatibili con l'applicazione e la connessione di telecomunicazione. Sarà cura dell'ENTE assicurare che i terminali utilizzati per fruire dei servizi siano dotati di misure di sicurezza e sistemi antivirus aggiornati adeguati a poter proteggere i file scaricati sul terminale o caricati dal terminale sulla piattaforma.

4.8 L'ENTE si impegna ad utilizzare i SERVIZI esclusivamente per gli scopi e attraverso i canali concordati contrattualmente.

4.9 L'ENTE deve attenersi ad adeguati standard di sicurezza tecnica ed organizzativa e garantire che nessun virus, trojan o altro programma dannoso proveniente dai suoi sistemi entri in quelli del FORNITORE. L'ENTE è inoltre responsabile del controllo del corretto utilizzo dei SERVIZI da parte dei suoi collaboratori e, in particolare, di quelli che sono autorizzati ad accedere alla PIATTAFORMA.

4.10 L'ENTE deve garantire che l'uso da parte del FORNITORE delle informazioni, dei dati e dei materiali da lui forniti non violi i diritti di terzi. Prima di fornire al FORNITORE le informazioni, i dati e i materiali corrispondenti, l'ENTE è tenuto a verificare se il FORNITORE abbia il permesso di utilizzare tali informazioni, dati e materiali nell'ambito delle prestazioni concordate in conformità al presente CONTRATTO e, se necessario, a fornire gli eventuali diritti d'uso necessari e ad ottenere il consenso di terzi. L'ENTE terrà indenne il FORNITORE da tutte le pretese di terzi che risultino da una violazione dei suddetti obblighi. L'indennizzo comprende anche i costi di ogni necessaria difesa legale.

4.11 L'ENTE si impegna, inoltre, ad osservare le seguenti disposizioni nell'utilizzo dei SERVIZI, in particolare:

a. il sistema di whistleblowing non può essere utilizzato per altri scopi, ad esempio non può essere utilizzato come piattaforma di scambio di file o informazioni che sono illegali o violano le norme legali applicabili;
b. le informazioni sulla PIATTAFORMA dell'ENTE, che possono essere accessibili pubblicamente, e la descrizione degli avvisi nel sistema di whistleblowing devono essere fattuali, oggettive e

accurate. Non devono violare alcun brevetto, diritto d'autore, marchio, diritto personale o altre posizioni giuridiche protette di terzi;

c. l'ENTE si impegna a non distribuire i seguenti contenuti attraverso il sistema di segnalazione o a renderli accessibili a terzi in qualsiasi altro modo:
   i. contenuti che siano pornografici, osceni, offensivi, volgari o altrimenti discutibili;
   ii. contenuti che rappresentano un rischio per la sicurezza come portatori di virus, trojan o altri programmi dannosi;
   iii. contenuti che siano discriminatori, razzisti, sprezzanti dei diritti umani, radicali, religiosi, xenofobi, nazionalsocialisti, pornografici o altrimenti sessualmente degradanti;
   iv. dichiarazioni o azioni di qualsiasi tipo che violino le disposizioni di legge;
d. l'ENTE si impegna a rispettare il Regolamento di Uso Accettabile allegato al presente CONTRATTO; in caso di modifica del regolamento da parte del fornitore lo stesso provvederà a darne comunicazione all'ENTE e a pubblicarne copia all'indirizzo: https://www.whistleblowing.it/documentazione-tecnica/.

4.12 Se l'ENTE viola gli obblighi che deve rispettare in virtù del presente CONTRATTO il FORNITORE ha il diritto di sospendere l'accesso ai SERVIZI e/o di cancellare l'account dell'ENTE e/o i contenuti che violano il CONTRATTO o la legge, o di modificarli a un livello ammissibile, di porre fine alla presente relazione contrattuale e/o di rifiutare all'ENTE una nuova registrazione. Qualsiasi pretesa dell'ENTE nei confronti del FORNITORE per tali misure è esclusa.

5. PROPRIETÀ INTELLETTUALE

5.1 Qualsiasi diritto di proprietà intellettuale riguardante la PIATTAFORMA e i SERVIZI sono posseduti o autorizzati dal FORNITORE e sono soggetti a copyright e ai diritti di proprietà intellettuale secondo le leggi italiane in materia e le convenzioni internazionali. L'ENTE acconsente a non rimuovere, alterare o nascondere qualsiasi evidenza di proprietà intellettuale che sia incorporata nella PIATTAFORMA e nei SERVIZI o che li accompagni, nonché a non riprodurre, modificare, adattare, produrre materiale derivato che si basi sull'eseguire, mostrare, pubblicare, distribuire, trasmettere, diffondere, vendere, autorizzare, o in qualsiasi altro modo sfruttare la PIATTAFORMA e i SERVIZI. Se l'ENTE dovesse violare il diritto di proprietà intellettuale, il FORNITORE potrebbe inibirgli l'uso dei SERVIZI e della PIATTAFORMA qualora lo ritenesse opportuno e appropriato. Il FORNITORE possiede tutti i diritti non espressamente garantiti con riguardo ai SERVIZI e alla PIATTAFORMA. L'ENTE acconsente a non usare, copiare e distribuire i SERVIZI in maniera diversa da quella espressamente definita in questa sede.

5.2 Conformemente al CONTRATTO e alle seguenti disposizioni, l'ENTE riceve il diritto semplice, non esclusivo e non trasferibile, limitato alla durata del CONTRATTO, di utilizzare i SERVIZI sottoscritti per sé stesso e per gli utenti autorizzati per i propri scopi.

6. GARANZIE E LIMITAZIONI DI RESPONSABILITÀ

6.1 Il FORNITORE s'impegna ad erogare i SERVIZI con le caratteristiche conformi a quelle indicate nelle schede descrittive del prodotto alla data di attivazione del prodotto medesimo, fatta salva la necessità di procedere ad aggiornamenti hardware e software in base a circostanze contingenti.

6.2 In ogni caso, il FORNITORE e i suoi sub-fornitori non saranno ritenuti responsabili di eventuali perdite o danni non ragionevolmente prevedibili.

6.3 L'ENTE si obbliga a tenere indenne e tutelare il FORNITORE e i suoi sub-fornitori da qualsiasi reclamo, causa o azione derivanti da o relativi all'utilizzo dei SERVIZI o alla violazione del presente CONTRATTO, comprese eventuali responsabilità o spese derivanti da reclami, perdite, danni, azioni legali, sentenze, spese processuali e legali.

6.4 L'utilizzo mediante web dei SERVIZI viene consentito nello stato in cui si trova, senza alcuna garanzia che le funzioni contenute e descritte nelle specifiche soddisfino le esigenze dell'ENTE o funzionino in tutte le combinazioni hardware, software e gestionali/aziendali che possono essere scelte per l'uso da parte dell'ENTE, il quale, prima della sottoscrizione del presente CONTRATTO, ha compiutamente controllato e valutato, sotto la sua personale responsabilità, la soddisfazione delle proprie esigenze. L'ENTE ha l'onere di controllare costantemente il software e verificare il risultato delle elaborazioni compiute tramite di esso e del cui utilizzo è esclusivamente responsabile. Il FORNITORE non assume alcuna obbligazione e non presta alcuna garanzia oltre quelle qui espressamente descritte. Resta espressamente esclusa qualsivoglia responsabilità del FORNITORE per danni diretti ed indiretti di qualsiasi natura che l'ENTE o terzi possano subire per effetto ed in conseguenza del presente CONTRATTO e verificatisi per causa non imputabile, anche indirettamente, al FORNITORE, ivi compresi quelli derivanti dall'uso o dal mancato uso delle procedure o da errori delle stesse, o quelli, senza limitazioni, per perdita o mancato guadagno, fermo dell'attività, perdite economiche o di informazioni, nonché per i malfunzionamenti o difetti relativi o causati dagli ambienti informatici o dai sistemi operativi sui quali operano i programmi.

6.5 Nei limiti massimi consentiti dalla legge, il FORNITORE è responsabile solo in caso di dolo e colpa grave. Ciò vale anche per il comportamento intenzionale o di grave negligenza dei rappresentanti e/o ausiliari dello stesso. Questa limitazione di responsabilità non si applica in caso di lesioni alla vita, all'integrità fisica o alla salute o in caso di responsabilità obbligatoria ai sensi della legge sulla responsabilità del prodotto.

6.6 La responsabilità per i danni è limitata ai danni prevedibili e tipici. Non rientrano quindi nella sfera di responsabilità del FORNITORE, eventi come forza maggiore, scioperi, misure ufficiali, guasti dei mezzi di trasmissione o altre interruzioni.

6.7 Salvo quanto espressamente previsto dal presente CONTRATTO, la responsabilità del FORNITORE è esclusa.

7. MIGLIORIE, AGGIORNAMENTO E SOSPENSIONE DEI SERVIZI

7.1 Il FORNITORE si impegna costantemente nella ricerca e miglioria continua dei propri SERVIZI: è possibile che vengano aggiunte o rimosse funzionalità o caratteristiche.

7.2 Il FORNITORE si riserva il diritto di ampliare, modificare o limitare le funzioni nella misura in cui ciò serva al progresso tecnico, sia necessario per evitare abusi o sia obbligato a farlo per legge e non garantisce che le nuove versioni abbiano identiche funzionalità delle versioni precedenti. Tali modifiche potranno essere introdotte in qualsiasi momento poiché il FORNITORE aggiorna continuamente i propri SERVIZI. Potranno essere altresì introdotte sulla base di un piano di evoluzione e sviluppo predefinito e di eventuali nuove specifiche tecniche e funzionali che nel tempo, a suo insindacabile giudizio, abbia giudicato utili o necessarie, o in base alla necessità di manutenzione o correzione di eventuali malfunzionamenti o anomalie che gli siano stati segnalati o comunque rilevati nell'uso dei SERVIZI. Per ogni rilascio di release primaria effettuato sui SERVIZI, il FORNITORE invierà comunicazione tramite la PIATTAFORMA, indicante la descrizione delle principali novità funzionali.

7.3 L'ENTE dovrà pertanto scrupolosamente verificare, con onere a proprio esclusivo carico, l'applicabilità dei nuovi aggiornamenti, e quindi a titolo esemplificativo, ma non esaustivo, si obbliga sin da ora a verificare le nuove funzionalità e se siano adatte ai propri scopi senza che eventuali inesattezze, mancanze e/o difetti possano far sorgere in capo al FORNITORE responsabilità anche a titolo di colpa lieve. L'ENTE esonera e manleva sin da ora il FORNITORE da ogni responsabilità per danni, di qualsivoglia natura, da ciò derivati e/o derivanti allo stesso e/o a terzi. Il FORNITORE si riserva inoltre il diritto insindacabile di modificare, sostituire, eliminare ed interrompere la distribuzione di uno o più SERVIZI e/o di cessarne gli aggiornamenti.

7.4 Il FORNITORE potrebbe altresì sospendere l'erogazione dei SERVIZI per effettuare aggiornamenti o attività di manutenzione. In tal caso, ne darà un congruo preavviso all'ENTE.

7.5 Previa eventuale comunicazione da inviarsi all'ENTE mediante posta elettronica, il FORNITORE potrà interrompere il collegamento in presenza di comprovati problemi di sicurezza e/o di garanzia di riservatezza. Il FORNITORE non potrà in ogni caso essere ritenuto responsabile per interruzioni di servizio non dipendenti dalla propria volontà quali, a mero titolo esemplificativo, l'interruzione o il cattivo funzionamento delle reti telefoniche, telematiche, elettriche, dei servizi di connettività offerti dai provider o dai gestori della rete Internet.

7.6 Il FORNITORE potrebbe altresì decidere di sospendere o interrompere i SERVIZI in risposta a circostanze impreviste fuori dal proprio controllo o in ottemperanza a un obbligo giuridico. Al verificarsi di tale condizione, ove possibile, l'ENTE verrà avvisato con preavviso ragionevole per consentire l'esportazione dei dati dai sistemi. In nessun caso il FORNITORE sarà ritenuto responsabile di ritardi e/o violazioni dovute a cause a lui non imputabili e/o discendenti da obblighi derivanti dalla legge, regolamenti, ordini, disposizioni amministrative promanate da qualsiasi autorità civile e/o militare, ente statale e/o locale, atti od omissioni dell'altra parte (e così a titolo esemplificativo ma non esaustivo: incendi, inondazioni, terremoti, scioperi, embarghi, guerre, sabotaggi). Il FORNITORE provvederà al salvataggio degli archivi, banche dati e ogni altra informazione presente nello spazio dedicato all'ENTE. Laddove, per cause non imputabili al FORNITORE si verifichi la distruzione dei dati presenti sui server, il FORNITORE stesso provvederà a ripristinarli dal più recente salvataggio

disponibile entro 72 (settantadue) ore lavorative dalla segnalazione dell'incidente, senza che l'ENTE possa avanzare alcuna pretesa o richiesta di risarcimento.

7.7 Il FORNITORE potrà, altresì, interrompere la fornitura dei SERVIZI in caso di inosservanza del presente CONTRATTO.

8. RESPONSABILITÀ DEI DATI

8.1 L'ENTE è totalmente responsabile dei dati inseriti nella piattaforma a lui riservata dal FORNITORE e delle eventuali segnalazioni ricevute e pertanto accetta, con la sottoscrizione del presente CONTRATTO, di esentare il FORNITORE da responsabilità di carattere civile e/o penale derivanti dall'archiviazione e dalla diffusione dei dati da esso inseriti che violino qualunque prescrizione di legge o di regolamento o qualsiasi provvedimento proveniente da un'Autorità amministrativa o dall'Autorità giudiziaria.

8.2 L'ENTE è responsabile della custodia delle credenziali di autenticazione per l'accesso ai dati erogati dai SERVIZI del FORNITORE al fine di evitare l'accesso ad altri soggetti non autorizzati.

8.3 L'utilizzo dei SERVIZI è consentito solo in base a quanto consentito dalla legislazione in vigore, comprese leggi, regolamenti e provvedimenti dell'Autorità Garante per la protezione dei dati personali.

9. DURATA DEL CONTRATTO

9.1 Il presente CONTRATTO ha durata di mesi 12 (dodici) decorrenti dalla data della sua sottoscrizione. Al termine del periodo di validità, il presente CONTRATTO si intende, salvo diversa ed espressa indicazione, ogni volta tacitamente e automaticamente rinnovato con durata annuale, a meno che una delle parti non provveda ad effettuare comunicazione di recesso, a mezzo Raccomandata A/R ovvero altro mezzo di comunicazione, anche elettronico, purché assistito da conferma del FORNITORE, con un anticipo di almeno 30 giorni sulla scadenza prevista.

10. RECESSO E RISOLUZIONE

10.1 Il FORNITORE ha il diritto di modificare il presente CONTRATTO in qualsiasi momento. L'ENTE sarà informato di queste modifiche con un congruo preavviso e in forma scritta (cartacea o elettronica). In questo caso l'ENTE avrà la facoltà di recedere prima della scadenza del termine di preavviso. In caso di mancato esercizio di tale diritto, le modifiche saranno considerate accettate. Qualora il FORNITORE sia impossibilitato a fornire il preavviso per cause imprevedibili e non influenzabili (come, ad esempio, interventi normativi), il FORNITORE ha il diritto di modificare il CONTRATTO anche senza il consenso dell'ENTE. L'ENTE ne sarà ugualmente informato per iscritto.

10.2 Le parti convengono che, qualora il FORNITORE intenda eliminare e/o interrompere la distribuzione di uno o più SERVIZI, l'ENTE avrà diritto di recedere dagli stessi; il recesso avrà effetto decorsi 20 (venti) giorni dalla ricezione della PEC.

10.3 Resta inteso che non costituiscono giusta causa di recesso la modifica e/o la sostituzione di uno o più SERVIZI.

10.4 Entrambe le parti avranno facoltà di recedere nei termini e secondo le modalità previste dall'art. 9.1.

10.5 Il FORNITORE si riserva di recedere dal CONTRATTO, sospendere o interrompere la fornitura dei SERVIZI all'ENTE in qualsiasi momento, nel caso in cui l'ENTE violi gli obblighi che deve rispettare in virtù del presente CONTRATTO (per esempio nel caso in cui non venga rispettato il Regolamento di Uso Accettabile). Qualsiasi pretesa dell'ENTE nei confronti del FORNITORE per tali misure è esclusa.

10.6 Il FORNITORE potrebbe inoltre interrompere la fornitura di SERVIZI all'ENTE in qualsiasi momento nel caso in cui la PIATTAFORMA sia attivata da un soggetto non titolato dall'ENTE stesso, nel caso in cui la destinazione d'uso della PIATTAFORMA non sia per la compliance anticorruzione di un ente pubblico e/o società controllata dallo stesso, nel caso in cui l'impiego della PIATTAFORMA comporti dei costi per l'utilizzatore finale corrisposti a terzi (es: società privata che rivendesse la piattaforma gratuita a un ente pubblico).

11. ASSISTENZA TECNICA E MANUTENZIONE

11.1 È esclusa, salvo diverso e specifico accordo, ogni forma di assistenza tecnica e manutenzione da parte del FORNITORE. Il FORNITORE, con un impegno di tipo best-effort, provvederà a rispondere alle richieste di chiarimenti eventualmente pervenute.

12. TRATTAMENTO DEI DATI PERSONALI

12.1 La fornitura dei SERVIZI è soggetta alla presa visione e accettazione dell'Informativa Privacy allegata al presente CONTRATTO.

12.2 L'ENTE, in qualità di titolare del trattamento, è tenuto a predisporre e a fornire agli interessati un'apposita informativa privacy che dettagli le informazioni richieste ai sensi degli articoli 13, ed eventualmente 14, del Regolamento (UE) 2016/679 ("GDPR").

12.3 Il FORNITORE sarà designato quale Responsabile del trattamento ai sensi dell'art 28 del GDPR e, a tal fine, sarà nominato mediante un apposito contratto o altro atto giuridico a norma del diritto dell'Unione Europea o degli Stati membri. Il FORNITORE si impegna, a sua volta, a nominare eventuali sub-fornitori come sub-responsabili del trattamento secondo le modalità previste dall'art. 28, comma 4, GDPR e a darne notizia all'ENTE.

12.4 I dati personali trattati ai soli fini della conclusione del presente CONTRATTO e della fornitura dei relativi SERVIZI sono quelli comunicati dall'ENTE al FORNITORE.

13. ACCORDO COMPLESSIVO

13.1 Il presente CONTRATTO costituisce l'unico integrale e complessivo CONTRATTO tra le parti con riferimento alla materia da esso disciplinata, e sostituisce qualsiasi precedente accordo, intesa, contratto o negozio, scritto o orale, che le parti possano aver stipulato in relazione al suo contenuto.

13.2 Il presente CONTRATTO si applica a tutti i SERVIZI eventualmente attivati anche successivamente al primo periodo di validità.

14. VALIDITÀ DEL CONTRATTO

14.1 Nel caso in cui qualcuna delle disposizioni del CONTRATTO – o parte di esso – sia ritenuta nulla, annullabile, invalida o inefficace dall'Autorità Giudiziaria, o comunque risulti o diventa integralmente o parzialmente priva d'effetto giuridico o inefficace, tale nullità, annullabilità, invalidità, o comunque inefficacia, non avrà effetto sulle altre disposizioni del CONTRATTO né, tanto meno, potrà determinare la nullità, annullabilità, invalidità o inefficacia dell'intero CONTRATTO.

14.2 La disposizione – o la parte di essa – ritenuta nulla, annullabile, invalida o inefficace dall'Autorità Giudiziaria, dovrà intendersi modificata, reinterpretata o integrata, nella misura e secondo il senso necessari a che la stessa possa essere ritenuta ammissibile per legge, e giudicata pienamente valida ed efficace dall'Autorità Giudiziaria, preservando nella maggior misura possibile la volontà delle parti come risultante dal CONTRATTO.

14.3 Entro i limiti consentiti dalla legge applicabile, le disposizioni del presente CONTRATTO che, per loro natura, portata o significato, sono da intendersi come a rimanere in vigore anche alla scadenza, a seguito dell'adempimento, della risoluzione o di qualsiasi altra forma di cessazione dell'efficacia del CONTRATTO, continueranno ad avere vigore e ad applicarsi anche a seguito della scadenza delle stesse.

15. LEGGE APPLICABILE E FORO COMPETENTE

15.1 Il presente CONTRATTO è regolato dalle leggi dello Stato Italiano. Con la sottoscrizione del presente CONTRATTO le parti escludono integralmente l'applicazione della Convenzione delle Nazioni Unite sui Contratti di Vendita Internazionale di Beni Mobili ("UN Convention on Contracts for the International Sale of Goods – CISG", Vienna, 11 aprile 1980).

15.2 Il FORNITORE può, a sua discrezione, rendere disponibile e/o sottoscrivere il presente CONTRATTO anche in una lingua diversa dall'italiano. La versione in lingua italiana del presente CONTRATTO sarà comunque sempre prevalente in tutte le ipotesi di controversie e/o nei casi di conflitto interpretativo rispetto alla versione tradotta in altra lingua.

15.3 Entro i limiti consentiti dalla legge applicabile, l'ENTE, con la sottoscrizione del presente CONTRATTO, conferma che esso venga stipulato tra professionisti e per scopi commerciali, e concorda che le disposizioni delle leggi a protezione dei consumatori o dei contraenti deboli non sono applicabili.

15.4 Per tutte le controversie relative al CONTRATTO, le parti riconoscono la competenza esclusiva del Foro di Milano.

AUTORIZZAZIONE AL TRATTAMENTO DI DATI PERSONALI

Redatto ai sensi dell'art. 28 del Regolamento (UE) 2016/679 e del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008

Documento aggiornato il 13 novembre 2024

TRA

con sede in

Codice Fiscale e P. IVA n.

in persona di

(di seguito "**Committente** " o il "**Titolare del Trattamento**"),

E

Whistleblowing Solutions I.S. S.r.l., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961 del legale rappresentante pro tempore Ing. Giovanni Pellerano (di seguito "**Fornitore** " o il "**Responsabile del Trattamento**"), (di seguito, congiuntamente, le "**Parti**")

PREMESSO CHE

I. Le Parti hanno sottoscritto un contratto avente ad oggetto la prestazione da parte del Fornitore di un servizio di whistleblowing digitale consistente in fornitura in outsourcing di una piattaforma di whistleblowing digitale (di seguito, "Contratto di servizi");
II. in virtù del Contratto di servizi il Fornitore esegue operazioni di trattamento dei Dati personali di seguito, "Dati Personali" di titolarità del Committente, e riferiti unicamente ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare l'acquisizione e l'archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali

e reati o che rivelino, tra l'altro, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche identificate o identificabili che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate art. 4, par. 1, nn. 1) e 2), del Regolamento (UE) 2016/679 (di seguito, "Regolamento");

III. il Fornitore dichiara e garantisce di possedere competenza e conoscenze tecniche in relazione alle finalità e modalità di trattamento, alle misure di sicurezza da adottare a garanzia della riservatezza, completezza ed integrità dei Dati Personali trattati, nonché in relazione alla normativa italiana ed europea in materia di protezione dei dati personali, e di possedere i requisiti di affidabilità idonei a garantire il rispetto delle disposizioni normative in materia;

IV. secondo quanto prescritto dal Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 e ss.mm.ii. relativo alle "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema" (di seguito, "Provvedimento"), è necessario attribuire al Responsabile del Trattamento le attività di valutazione, designazione, verifica delle attività e registrazione degli accessi degli amministratori di sistema;

V. il Titolare del Trattamento ha condotto una positiva valutazione della idoneità e qualificazione del Responsabile del Trattamento atta a soddisfare, anche sotto il profilo della sicurezza del trattamento, i requisiti di cui alla normativa applicabile (artt. 28 e ss. del Regolamento) e intende designare il Fornitore quale Responsabile del Trattamento dei Dati Personali derivante dal Contratto di servizi.

Tutto quanto sopra premesso, tenuto conto delle reciproche promesse e degli accordi intercorsi, le Parti convengono quanto segue:

1. PREMESSE

1.1. Le premesse costituiscono parte integrante ed essenziale del presente atto.

2. OGGETTO

2.1. Con la sottoscrizione del presente atto il Committente nomina il Fornitore, che accetta, Responsabile del Trattamento in relazione alle operazioni di trattamento dei Dati Personali poste in essere ai soli fini dell'esecuzione del Contratto di servizi. Tale nomina non comporta il diritto ad alcuna remunerazione.

2.2. I compiti assegnati al Fornitore sono esclusivamente quelli resi necessari dalle attività connesse all'esecuzione del Contratto di servizi.

3. OBBLIGHI DEL TITOLARE DEL TRATTAMENTO

3.1. Qualora nell'ambito delle operazioni di trattamento dei Dati Personali occorrano eventuali istruzioni aggiuntive al fine di adeguarsi alla normativa in materia di protezione dei dati, il Committente trasmetterà ulteriori istruzioni al Fornitore in merito alle finalità, modalità e procedure per l'utilizzo e il trattamento dei Dati Personali, e concorderà con il Fornitore le misure tecniche ed organizzative più idonee.

4. OBBLIGHI DEL RESPONSABILE DEL TRATTAMENTO

4.1. Ai fini di un corretto trattamento dei Dati Personali, il Fornitore si impegna a:

a. svolgere qualsiasi operazione di trattamento dei Dati Personali in conformità ai principi e alla regolamentazione previsti dalla normativa vigente in materia di protezione dei dati personali;
b. eseguire fedelmente ed esclusivamente le istruzioni impartite dal Titolare del Trattamento, evitando attività di trattamento non conformi alle predette istruzioni o volte a perseguire finalità diverse da quelle correlate all'esecuzione del Contratto di servizi;
c. non effettuare copie dei Dati Personali diverse da quelle strettamente necessarie alla corretta esecuzione del Contratto di servizi;
d. garantire il pieno rispetto degli obblighi di cui il Fornitore, quale Responsabile del Trattamento, è tenuto in virtù della normativa vigente;
e. fuori dai casi strettamente necessari per l'erogazione dei Servizi, non divulgare o rendere noti a terzi i Dati Personali e adottare le misure organizzative e tecniche necessarie per assicurare la massima riservatezza dei Dati Personali acquisiti e utilizzati nello svolgimento delle attività oggetto della presente designazione;
f. garantire che l'accesso ai Dati Personali da parte del personale avvenga solo sulla base del principio di stretta necessità, provvedendo a individuare e designare quali incaricati del trattamento, anche ai fini di cui all'art. 32 del Regolamento, le persone fisiche (dipendenti e/o collaboratori) autorizzate al trattamento dei dati personali per le suddette finalità, impegnando gli stessi con idonei vincoli di riservatezza;
g. formare adeguatamente il personale addetto all'esecuzione del Contratto di servizi fornendo loro istruzioni precise e vigilando sulla loro osservanza;
h. collaborare con il Committente per l'attuazione di qualsiasi misura che si renda strettamente necessaria al fine di garantire la conformità del trattamento dei Dati Personali con la normativa applicabile;
i. effettuare, ai sensi dell'art. 32 del Regolamento, regolari analisi dei rischi per adottare misure tecniche organizzative adeguate rispetto alle prescrizioni di legge in materia di protezione dei dati personali, di informatica giuridica e amministrazione digitale di cui al CAD e disciplina applicabile, nonché dei provvedimenti del Garante per la Protezione dei Dati Personali e dell'Agenzia per l'Italia Digitale (AGID) o altra Autorità di controllo competente;
j. stabilire, nell'ambito della propria organizzazione, i c.d. mezzi non essenziali, quali misure di sicurezza di dettaglio, e sulla base delle proprie competenze

tecniche specifiche, collaborare, anche manifestando un'autonomia propositiva, nell'adozione di misure adeguate e nella verifica sistematica dell'efficacia delle stesse tramite una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento;

k. effettuare analisi che esplicitino i rischi e le eventuali possibili misure di attenuazione degli stessi da proporre al Titolare del Trattamento, propedeutiche a valutazioni di impatto, informando quest'ultimo e fornendo copia degli elaborati finali;
l. mantenere informato il Committente riguardo alle operazioni di trattamento trasmettendo un rapporto scritto sull'attività svolta in esecuzione dei compiti attribuiti con il presente atto, con particolare riguardo, ma non esclusivamente, alle misure di sicurezza adottate, nonché riguardo a qualsiasi circostanza o criticità eventualmente riscontrata;
m. informare il Committente, tempestivamente e non oltre le 48 ore dal momento in cui ne è venuto a conoscenza, di qualsiasi violazione o rischio di violazione concernente i Dati Personali di cui il Fornitore è venuto a conoscenza nello svolgimento dei Servizi e collaborare, a proprie spese, con il Committente per attuare qualsiasi misura che si renda strettamente necessaria al fine di garantire la conformità del trattamento dei Dati Personali con la normativa applicabile;
n. adottare le misure di sicurezza previste dall'articolo 7 del presente atto
o. reindirizzare verso il Titolare del Trattamento per gli obblighi di dar seguito ad eventuali domande di esercizio dei diritti delle persone interessate di cui agli articoli da 12 a 23 del Regolamento.

4.2. Con riferimento al trattamento dei Dati Personali svolti con l'ausilio di strumenti elettronici per la prestazione dei Servizi e la gestione del database per conto del Committente, nel rispetto del Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008 così come modificato dal Provvedimento del Garante per la Protezione dei Dati Personali del 25 giugno 2009, il Responsabile del Trattamento si impegna ad attuare le seguenti misure:

a. procedere alla designazione individuale degli amministratori di sistema o figura equivalente, previa valutazione delle caratteristiche di esperienza, capacità e affidabilità del soggetto designato, in grado di garantire il pieno rispetto della normativa italiana in materia di protezione dei dati personali, ivi compreso il profilo relativo alla sicurezza;
b. individuare, per ciascun amministratore di sistema designato, o figura equivalente, gli ambiti di operatività consentiti in base al profilo di autorizzazione assegnato;
c. conservare un elenco aggiornato degli estremi identificativi delle persone fisiche preposte quali amministratori di sistema o figura equivalente e, su richiesta, mettere tale elenco a disposizione del Committente e/o delle autorità competenti;
d. verificare, con cadenza almeno annuale, l'operato degli amministratori di sistema o figure equivalenti in modo da controllarne la rispondenza alle misure

organizzative, tecniche e di sicurezza per il trattamento dei Dati Personali previste dalle norme vigenti;

e. adottare sistemi idonei alla registrazione degli accessi logici ai sistemi di elaborazione e agli archivi elettronici da parte degli amministratori di sistema o figure equivalenti; le registrazioni dovranno essere conservate per un congruo periodo, comunque non inferiore ai sei mesi.

5. AFFIDAMENTO A TERZI

5.1. Il Fornitore si impegna a prevedere nel contratto con il subfornitore garanzie e obblighi analoghi a quelli di cui al presente atto. Il Responsabile del Trattamento dichiara di avvalersi dei Subresponsabili indicati nell'Allegato A. Con la sottoscrizione del presente atto, i Subresponsabili indicati nell'Allegato A si intendono approvati dal Titolare del Trattamento. Il Fornitore dichiara che i Subresponsabili hanno capacità e competenze per mettere in atto misure tecniche e organizzative idonee a garantire il rispetto delle disposizioni della vigente normativa sulla protezione dei dati personali e che sono stati contrattualmente vincolati al rispetto degli stessi obblighi in materia di protezione dei dati personali assunti dal Responsabile del Trattamento nei confronti del Titolare del Trattamento. Qualora il Responsabile del Trattamento intenda sostituire i Subresponsabili indicati nell'Allegato A, dovrà informare il Titolare del Trattamento preventivamente e per iscritto, con un preavviso di 60 giorni. Resta ferma la possibilità di derogare al termine di preavviso, nel caso siano necessarie operazioni di mitigazione di un disastro imputabile al subfornitore. Il Fornitore dichiara e garantisce che eventuali, nuovi, Subresponsabili presenteranno almeno le stesse caratteristiche e garanzie dei Subresponsabili indicati nell'Allegato A e saranno vincolati contrattualmente al rispetto dei medesimi obblighi in materia di protezione dei dati personali assunti dai Subresponsabili.

6. DURATA - CESSAZIONE

6.1. L'efficacia del presente atto decorre dalla data di sottoscrizione dello stesso ad opera di entrambe le Parti sino alla cessazione, per qualsiasi causa intervenuta, del Contratto di servizi.

6.2. All'atto della cessazione del Contratto di servizi il Fornitore dovrà cessare qualsiasi operazione di trattamento dei Dati Personali e restituire al Committente tutti gli eventuali Dati Personali trattati ai fini dell'esecuzione del Contratto di servizi di cui il Fornitore dovesse disporre (es. anagrafiche degli interessati, dati di contatto degli interessati) o, su richiesta del Committente, provvedere alla loro distruzione, fornendone apposita attestazione, eccettuate eventuali esigenze di loro conservazione in adempimento di obblighi normativi di cui andrà data contestuale attestazione al Committente.

7. MISURE DI SICUREZZA

7.1. Con riferimento alle operazioni di trattamento dei Dati Personali necessarie ai fini della esecuzione del Contratto di servizi, il Fornitore dichiara e garantisce di mantenere,

ogni e qualsiasi misura di sicurezza idonea a prevenire i rischi di distruzione, perdita, anche accidentale, dei Dati Personali nonché di accesso non autorizzato o trattamento illecito dei medesimi come previsto nel Contratto di servizi e che tali misure sono conformi anche alle misure di sicurezza necessarie e conformi ai principi di cui all'art. 32 del Regolamento, nonché ogni altra misura obbligatoria di legge.

7.2. Il Fornitore si impegna a verificare regolarmente l'idoneità delle misure adottate.

8. CONTROLLI

8.1. Il Fornitore riconosce e accetta che il Committente, nell'ambito dei poteri e obbligazioni ad esso spettanti in quanto Titolare del Trattamento, possa controllare le operazioni di trattamento dei Dati Personali svolte dal Fornitore, come anche le misure di sicurezza attuate da quest'ultimo per le finalità di cui al presente atto, anche mediante appositi audit da concordarsi preventivamente nel rispetto delle reciproche esigenze lavorative.

9. DISPOSIZIONI FINALI

9.1. Con la sottoscrizione del presente atto, il Responsabile del Trattamento accetta la nomina e, in ottemperanza di quanto disposto dal Regolamento (UE) 2016/679 e dal Provvedimento del Garante per la Protezione dei Dati Personali del 27 novembre 2008, si impegna ad adempiere alla normativa pro tempore vigente in materia di protezione dei dati personali nonché di attenersi alle istruzioni impartite dal Titolare del Trattamento per mezzo del presente atto.

9.2. Ciascuna Parte è responsabile per l'adempimento dei propri obblighi previsti dal presente atto e dalla normativa pro tempore vigente in materia di protezione dei dati personali, di cui la documentazione contrattuale e tecnica costituisce parte integrante.

Whistleblowing Solutions I.S. S.r.l. preso atto di quanto previsto nel presente atto di nomina e dalla normativa vigente, dichiara di accettare l'incarico di Responsabile del Trattamento.

Luogo e Data

_____
Il Titolare del trattamento

_____
Il Responsabile del trattamento
Whistleblowing Solutions Impresa Sociale S.r.l.
Legale Rappresentante, Giovanni Pellerano

ALLEGATO A

Elenco dei Subresponsabili di cui si avvale il Responsabile del Trattamento al momento della sottoscrizione dell'Autorizzazione al Trattamento

DENOMINAZIONE, SEDE E DATI DI CONTATTO DEL SUBRESPONSABILE	ATTIVITÀ DI TRATTAMENTO DEMANDATE AL SUBRESPONSABILE	LUOGO DEL TRATTAMENTO
SEEWEB S.R.L	ARCHIVIAZIONE HOSTING CLOUD IASS	MILANO FROSINONE (BACKUP)
TRANSPARENCY INTERNATIONAL ITALIA	SUPPORTO UTENTI AMMINISTRATORE DI SISTEMA	MILANO

2025

Valutazione d’impatto sulla protezione dei dati (ex Art. 35 GDPR)

WHISTLEBLOWING

TEAM DPO

morolabs

.

Sommario

Introduzione 3
Campo di applicazione 3
Scopo 3
Destinatari 3
Normativa di riferimento 3
Che cosa è la PIA/DPIA (fonte WP248) 3
Cosa prevede il Regolamento per la PIA/DPIA (fonte WP248) 4
Quando è necessaria la DPIA 5
Modalità 7
Fasi PIA/DPIA 7
Fase 1: Elencare e raggruppare le attività di trattamento dei dati 7
Fase 2: Rispondere al questionario di valutazione dei valori soglia 8
Fase 4: Rispondere al questionario sulla PIA/DPIA 8
Fase 5: Identificare i rischi principali per la sicurezza 8
Fase 6: Come mitigare i rischi 8
Fase 7: Registrare l'implementazione 9
Consultazioni con l'Autorità di controllo 9
Revisione periodica PIA/DPIA 9
SCHEDA DPIA RELATIVA AL TRATTAMENTO 10

.

Introduzione

La Valutazione d'impatto sulla protezione dei dati o DPIA è un procedimento obbligatorio ai sensi del Regolamento (UE) 2016/679 quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate, a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori.

Lo strumento è coerente con il principio della responsabilizzazione o *accountability* introdotto dal GDPR al comma 2, Art. 5. Il Titolare è chiamato non solo a rispettare le norme del Regolamento ma anche all' attestazione formale dell'adozione delle misure (non più minime ma) idonee a garantire il rispetto di tali prescrizioni. La DPIA è quindi una procedura che permette la valutazione e soprattutto la dimostrazione della conformità alle norme in materia di protezione dei dati personali.

Campo di applicazione

Il campo di applicazione della presente Valutazione d'Impatto sulla Protezione dei Dati (PIA/DPIA) è relativo alla gestione del Whistleblowing, ai sensi del D.lgs. n. 24/2023.

Scopo

Ai sensi dell'art. 35 del Regolamento (UE) 2016/679 la PIA/DPIA è effettuata ogniqualvolta *un trattamento, allorché prevede in particolare l'uso di nuove tecnologie* (come nel caso di specie)*, 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*.

Destinatari

Destinatari di questo documento sono la Direzione, il Responsabile della Protezione dei Dati e il Gruppo di progetto GDPR; nei casi previsti, l'Autorità Garante può richiederne l'ostensione.

Normativa di riferimento

- Regolamento (UE) 2016/679 o GDPR - Articolo 35
- GDPR considerando 75, 84, 89, 90, 91, 92, 93
- WP 248 - 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
- Disposizioni e prescrizioni dell'Autorità Garante per la protezione dei dati personali

Che cosa è la PIA/DPIA (fonte WP248)

Una DPIA consiste in una procedura finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità, e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali (attraverso la valutazione di tali rischi e la definizione delle misure idonee ad affrontarli).

La DPIA è uno strumento importante in termini di responsabilizzazione (*accountability*) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del GDPR, ma anche a dimostrare l'adozione di misure idonee a garantire il rispetto di tali prescrizioni (art. 24 GDPR).

.

In altri termini, la DPIA è una procedura che permette di realizzare e dimostrare la conformità con le norme.

In base al Regolamento, l'inosservanza degli obblighi concernenti la DPIA può comportare sanzioni da parte della Autorità Garante della protezione dei dati personali. Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (art. 35, paragrafi 1 e 3-4), lo svolgimento non corretto di una DPIA (art. 35, paragrafi 2 e 7-9) o la mancata consultazione presso l'Autorità ove ciò sia necessario (art. 36, paragrafo 3, lettera e)) possono comportare sanzioni amministrative pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore.

Cosa prevede il Regolamento per la PIA/DPIA (fonte WP248)

Il regolamento impone ai titolari di mettere in atto misure idonee a garantire ed essere in grado di dimostrare l'osservanza del Regolamento stesso, tenendo conto, fra gli altri, dei "*rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche*" (art. 24, paragrafo 1). L'obbligo di condurre una DPIA, in determinate circostanze, deve essere collocato nel contesto del più generale obbligo imposto ai titolari di gestire correttamente i rischi connessi al trattamento di dati personali.

Per "rischio" si intende uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate in termini di probabilità e impatto (o gravità). La "gestione del rischio" è definita come l'insieme coordinato delle attività finalizzate a guidare e monitorare una organizzazione nei riguardi di tale rischio.

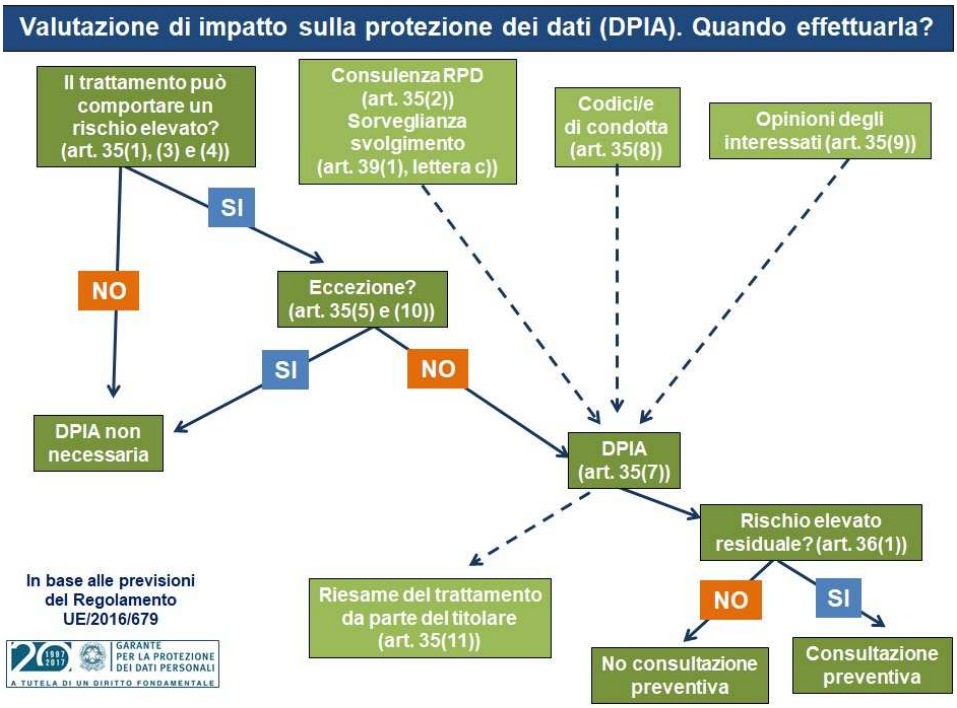
L'art. 35 del regolamento menziona la probabilità di un rischio elevato "per i diritti e le libertà delle persone fisiche".

Come già chiarito dal Gruppo di lavoro "Articolo 29" nella "Dichiarazione" sull'approccio basato sul rischio nel contesto giuridico della protezione dei dati, il riferimento ai "diritti e le libertà" degli interessati va inteso in primo luogo come relativo al diritto alla privacy, ma può riguardare anche altri diritti fondamentali quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

Coerentemente con l'approccio basato sul rischio che riforma il Regolamento rispetto alle normative precedenti, non è obbligatorio condurre una DPIA per ogni singolo trattamento. Viceversa, la DPIA è obbligatoria solo se una determinata tipologia di trattamenti *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (art. 35, paragrafo 1). Tuttavia, la semplice circostanza per cui non siano soddisfatte le condizioni che generano un obbligo di condurre la DPIA non riduce in alcun modo l'obbligo più generale cui sono sottoposti i titolari relativamente alla messa in atto di tutte le misure finalizzate a gestire in modo idoneo i rischi per i diritti e le libertà degli interessati. Nella pratica, ciò significa che i titolari devono valutare in modo continuativo i rischi connessi con i trattamenti, in modo da individuare le situazioni in cui una determinata tipologia di trattamenti "*può presentare un rischio elevato per i diritti e le libertà delle persone fisiche".*

La figura seguente illustra i principi fondamentali concernenti la DPIA in base al GDPR:

.



Quando è necessaria la DPIA

L'art. 35 del GDPR introduce l'obbligatorietà della Valutazione di impatto per i trattamenti che presentino rischi elevati per i diritti e le libertà delle persone fisiche, e in virtù della natura, l'oggetto, il contesto e le finalità dello stesso. Riuscire a identificare e discriminare caso per caso al fine di stabilire l'obbligatorietà o meno della valutazione non sempre risulta un'operazione semplice ed immediata, soprattutto se basata soltanto sulle basi previste dal Regolamento. Il Titolare, coadiuvato dal DPO, effettua una prevalutazione basandosi sulle informazioni essenziali già riportate nel Registro delle attività di trattamento al fine di valutare l'opportunità e/o la necessità di procedere o meno ad una DPIA.

Sempre l'art. 35 comma 3 riporta i casi per i quali si deve procedere tassativamente alla esecuzione della procedura di valutazione, ovvero:

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.

Alcune tipologie di trattamenti effettuati rientrano immediatamente in una delle casistiche per cui non è necessario procedere con un approfondimento. Ma vi sono molte situazioni intermedie e particolarmente complesse che hanno spinto l'Autorità a illustrare in modo più specifico cosa rientra nell'obbligo.

Il chiarimento interpretativo dell'Autorità Garante riportato in Allegato 1 al Provvedimento n. 467 dell'11 ottobre 2018 [doc. web n. 9058979] (Pubblicato sulla Gazzetta Ufficiale n. 269 del 19 novembre 2018) dove sono indicate le tipologie di trattamenti, soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto, di seguito riportate:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”.
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull’esercizio di un diritto fondamentale (quali i dati sull’ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell’interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).
5. Trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l’uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il Wi-Fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l’incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).
10. Trattamenti di categorie particolari di dati ai sensi dell’art. 9 oppure di dati relativi a condanne penali e a reati di cui all’art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell’attività di trattamento.

Altra doverosa considerazione, viste anche le dimensioni dell’Organizzazione, è la definizione di larga scala che, rispetto ai seguenti parametri:

a. il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
b. il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
c. la durata, ovvero la persistenza, dell'attività di trattamento;

.

d. la portata geografica dell'attività di trattamento.

Modalità

Il regolamento fissa le caratteristiche basilari di una PIA/DPIA all'art. 35, paragrafo 7, e nei considerando 84 e 90:

- una descrizione [sistematica] dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per:
  - affrontare i rischi
  - dimostrare la conformità al regolamento.

La figura seguente illustra il processo iterativo generale relativo alla conduzione di una DPIA

Fasi PIA/DPIA

Fase 1: Elencare e raggruppare le attività di trattamento dei dati

Il Responsabile della Protezione dei Dati ha il compito di valutare quali trattamenti sottoporre alla procedura di PIA/DPIA in funzione della tipologia e soprattutto dei rischi per gli interessati.

Nel registro della Valutazione d'impatto sulla Protezione dei Dati sono inserite le registrazioni relative alle attività di analisi delle situazioni al fine di comprendere se è necessario o meno procedere con la consultazione presso l'Autorità Garante.

È possibile eseguire una singola valutazione contemporaneamente per diverse attività di trattamento dei dati, se tali attività di trattamento presentano rischi elevati simili. Il Responsabile della Protezione dei Dati decide quali attività di trattamento dei dati saranno valutate insieme.

Fase 2: Rispondere al questionario di valutazione dei valori soglia

Il Responsabile della Protezione dei Dati deve rispondere a tutte le domande per ciascuna attività di trattamento dei dati con l'aiuto di persone responsabili per ciascuna attività di trattamento dei dati.

Queste domande sono necessarie per determinare se un'attività di trattamento può comportare un rischio elevato per i diritti e le libertà delle persone fisiche.

Fase 3: Decidere se è necessaria la PIA/DPIA

Il Responsabile della Protezione dei Dati determinerà se un'attività di trattamento dei dati deve essere analizzata attraverso la valutazione dei seguenti aspetti:

1. Il trattamento prevede la raccolta, uso, conservazione o condivisione di dati sensibili dei residenti dell'Unione Europea?
2. Il trattamento prevede utilizza dati personali per prevedere preferenze personali, ubicazione movimento di persone, situazione finanziaria, salute o rendimento lavorativo dei residenti nell'Unione Europea?
3. Il trattamento aiuta a prendere decisioni che possono avere un impatto significativo sugli individui, come negazione del credito, rifiuto dei servizi, ecc.?
4. Il trattamento prevede comporta un monitoraggio sistematico degli spazi pubblici su larga scala?
5. Sono presenti altri rischi associati con il trattamento per i diritti e le libertà delle persone?

È sufficiente rispondere positivamente ad una sola delle risposte precedenti che risulta necessario procedere con la PIA/DPIA.

Anche se le risposte a tutte le domande nel questionario sono "No", il Responsabile della Protezione dei Dati può decidere di eseguire la Valutazione d'impatto sulla Protezione dei Dati se l'organizzazione ha bisogno di avere una visione più chiara dei rischi che incombono sui dati.

Fase 4: Rispondere al questionario sulla PIA/DPIA

Per ciascuna attività di trattamento dei dati in cui sia richiesta la Valutazione d'impatto sulla Protezione dei Dati, il Responsabile della Protezione dei Dati deve compilare il questionario sulla Valutazione d'Impatto sulla Protezione dei Dati nel Registro delle Valutazioni d'Impatto sulla Protezione dei Dati. Tutti gli elementi obbligatori devono essere inseriti.

Lo scopo di queste domande è ottenere una descrizione sistematica delle attività di redazione ed elaborazione.

Fase 5: Identificare i rischi principali per la sicurezza

Una volta che il Responsabile della Protezione dei Dati ha completato il questionario sulla Valutazione d'impatto sulla Protezione dei Dati, deve utilizzare i risultati per identificare ed elencare i principali rischi per la sicurezza associati all'attività di trattamento in questione.

In particolare, il Responsabile della Protezione dei Dati deve prendere in considerazione i rischi derivanti dal trattamento dei dati personali, come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali.

Fase 6: Come mitigare i rischi

Una volta identificati ed elencati i rischi chiave, il Responsabile della Protezione dei Dati deve formulare un piano di mitigazione e inserirlo nel questionario. Le seguenti informazioni devono essere specificate:

- Misure protettive che devono essere implementate
- Responsabilità per l'implementazione
- Scadenze per l'implementazione

.

Fase 7: Registrare l'implementazione

Una volta implementata una protezione, il Responsabile della Protezione dei Dati deve registrarla nel questionario sulla Valutazione d'impatto sulla Protezione dei Dati sotto la colonna “Registrazione del Completamento”.

Consultazioni con l’Autorità di controllo

Se i risultati della Valutazione d'Impatto sulla Protezione dei Dati indicano che l’attività di trattamento dei dati può presentare un rischio elevato anche nel caso siano state implementate misure di sicurezza, il Responsabile della Protezione dei Dati procede con la consultazione presso l’Autorità di controllo prima dell’inizio del trattamento dei dati.

In questo caso, il Responsabile della Protezione dei Dati dovrà fornire all’Autorità di controllo le seguenti informazioni:

- Responsabilità del Titolare del trattamento, del contitolare (o contitolari) e del Responsabile
- Finalità e mezzi che saranno utilizzati per il trattamento
- Misure di sicurezza implementate per proteggere i dati
- Informazioni di contatto del Responsabile della Protezione dei Dati, e
- Risultati della Valutazione d'impatto sulla Protezione dei Dati

Revisione periodica PIA/DPIA

Il Responsabile della Protezione dei Dati deve riesaminare la PIA/DPIA in uno qualsiasi dei seguenti casi:

- Se i rischi relativi alle attività di trattamento dei dati sono modificati
- Se c’è un cambiamento significativo nelle attività di trattamento dei dati
- Se c'è un cambiamento nei requisiti legali
- Se un'azienda agisce come Responsabile e il Titolare richiede una revisione della PIA/DPIA

.

SCHEDA DPIA RELATIVA AL TRATTAMENTO

Informazioni generali del trattamento	
Denominazione del trattamento	**SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)**
Trattamenti cui si riferisce	Protezione dei dati personali delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'Organizzazione, di cui siano venute a conoscenza nel contesto lavorativo nel quale operano, ai sensi del D.lgs. n. 24/2023 (c.d. *whistleblowing*).
Descrizione del trattamento	La segnalazione interna può essere effettuata con una delle seguenti modalità, in ottemperanza all'art. 4, co. 3, del D.lgs. 24/2023: a) in forma scritta, tramite **piattaforma informatica** disponibile sul portale web istituzionale della **Provincia di Ancona** al link https://amministrazionetrasparente.provincia.ancona.it/L190/?idSezione=54141 b) – raggiungibile dall'interno della sezione Amministrazione Trasparente, sottosezione "Altri Contenuti/Prevenzione della Corruzione". In esito all'inoltro della segnalazione, il sistema rilascia un codice identificativo da utilizzare per i successivi accessi al fine di monitorare lo stato di avanzamento dell'istruttoria. L'applicativo informatico utilizza un protocollo di crittografia che garantisce la tutela della riservatezza dell'identità del segnalante, della/e persona/e coinvolta/e, delle persone comunque menzionate nella segnalazione, nonché l'integrità e la non violabilità del contenuto della segnalazione e della documentazione ivi allegata; c) mediante un **incontro diretto**, su richiesta della persona segnalante, con il Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**, debitamente verbalizzato previo consenso dell'interessato. I canali di segnalazione interna sono progettati in modo da consentire l'accesso alle segnalazioni solo da parte del personale espressamente autorizzato a trattare i dati inerenti alle medesime ai sensi degli artt. 28, 29 e 32, par. 4, del Regolamento (UE) 2016/679 e dell'art. 2-quaterdecies del D.lgs. 196/2003 ss.mm.ii.
Natura del trattamento	Registrazione, conservazione, consultazione, comunicazione, limitazione, cancellazione o distruzione.
Ambito di applicazione, contesto	Gestione delle segnalazioni – *Whistleblowing.*
Finalità del trattamento	Attività istituzionale.
Dati personali	Riferimenti segnalante e segnalati, eventuali notizie di violazioni.
Destinatari e autorizzati	Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**.
Periodo di conservazione	Pari a 5 anni. Le segnalazioni interne 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.
Asset coinvolti (hardware, software, reti,	Piattaforma per la gestione informatizzata della segnalazione: https://amministrazionetrasparente.provincia.ancona.it/L190/?idSezione=54141

canali cartacei o di trasmissione cartacea)	
Codici di condotta adottati (arti. 35, par. 8)	N/A Non è al momento prevista l'adozione di specifici Codici di condotta.
Motivo della redazione della DPIA	Art. 35 par. 3 lett. a) e c) GDPR; Provvedimento dell'Autorità Garante n° 467/2018; Art. 13, comma 6 del D.lgs. 24/2023 prevede obbligatoriamente la DPIA; Rischio elevato per i diritti e le libertà degli interessati.
DPIA correlate / versioning	Prima redazione – v. 1.0
Valutazione delle misure atte a garantire necessità e proporzionalità del trattamento (art. 35, paragrafo 7, lettera b)	
Finalità determinate, esplicite e legittime	*Scopo*: facilitare la segnalazione garantendo al contempo il necessario livello di riservatezza al fine di tutelare il segnalante adottando tutte le misure tecniche e organizzative necessarie. *Trasparenza*: informativa privacy in forma breve (sulla piattaforma) e in forma più estesa pubblicata sul sito web istituzionale e reperibile nella regolamentazione specifica. *Precisazione della finalità*: espressa nell'informativa e DPIA pubblicata sul sito web istituzionale.
Liceità del trattamento (art. 6; art. 9 GDPR e art. 2-sexies D.lgs. 196/03)	Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento: • Art. 6 par. 1 lettera c); • Art. 9 par. 2 lettera g); • Art. 13 del D.lgs. 24/2023.
Adeguatezza, pertinenza e non eccedenza (art. 5, par. 1, lettera c);	In conformità a quanto previsto dall'art. 13, comma 2 del D.lgs. 24/2023, i dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente in conformità a quanto previsto dall'art. 13 del D.lgs. 24/2023. Nella form di acquisizione della segnalazione pubblicata in **piattaforma software** è utilizzato l'insieme minimo delle informazioni necessarie alle finalità della gestione delle segnalazioni stesse; in particolare, l'utente provvede ad inserire i dati utilizzando i campi disponibili come Nome, Cognome, Ruolo dell'utente che effettua la registrazione, i dati relativi all'ente (nome, indirizzo, CF e PI) ed eventualmente dei soggetti, interni o esterni, coinvolti nella segnalazione. La piattaforma software utilizzata permette di raccogliere le segnalazioni secondo i migliori questionari predisposti nell'ambito del *whistleblowing* messi a punto da "*Transparency International Italia*" in relazione alla normativa vigente in materia, ulteriormente ridotti nei campi obbligatori. Nel rispetto del principio del *privacy by design* tutti gli elementi della catena tecnologica utilizzati nella costituzione del sistema, quali l'applicativo software GlobaLeaks, i log di sistema e del firewall

	sono configurati per non registrare, o comunque mantenere registrati soltanto per pochi istanti, alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo software GlobaLeaks vede abilitata oltre alla possibilità di navigazione anonima del browser senza accettazione di cookie, anche la navigazione tramite "*Tor Browser*" al fine di garantire un livello di anonimizzazione al passo con lo stato dell'arte della ricerca tecnologica in materia. Negli eventuali **incontri diretti** con il Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona** sono attuate accortezze similari durante la verbalizzazione.
Esattezza e aggiornamento dei dati (art. 5, par. 1, lettera d))	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. I dati personali possono essere tempestivamente cancellati o rettificati qualora, nel corso dell'istruttoria, risultassero inesatti rispetto alle finalità per le quali sono trattati («esattezza») in conformità a quanto previsto dall'art. 13 del D.lgs. 24/2023. Anche nel caso della segnalazione con incontro diretto l'esattezza e l'eventuale aggiornamento dei dati rimangono in campo al soggetto segnalante.
Limitazione della conservazione (*Retention*) (art. 5, par. 1, lettera e))	Le segnalazioni interne 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. Le segnalazioni scadute sono cancellate con procedura automatica in modalità sicura, non recuperabile.
Valutazione delle misure atte a garantire i diritti degli interessati[1]	
Informazioni fornite all'interessato (artt. 12, 13, 14)	Informativa sul sito web istituzionale in ottica stratificata e nella form iniziale di acquisizione delle segnalazioni in piattaforma applicativa. Per la segnalazione con incontro diretto la dovuta informativa è fornita dal Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona**.
Accesso (art. 15) e Portabilità dei dati (art. 20)	Diritto di accesso garantito al soggetto segnalante tramite codice rilasciato post invio della segnalazione. Tenendo sempre in debito conto la tutela del soggetto segnalante, l'eventuale esercizio di altri diritti previsti dall'ordinamento europeo e nazionale (segnatamente l'accesso ai documenti amministrativi, l'accesso civico e l'accesso ai dati personali, cfr. art. 12, comma 8, del Decreto D.lgs. 24/2023, in riferimento agli artt. 22 e ss. della l. n. 241/1990 e all'art. 5 e ss. del d.lgs. 33/2013, nonché art. 13, comma 3, del Decreto, in riferimento agli artt. 15-22 del Regolamento e all'art. 2-undecies del Codice) è sottoposto a deroghe e limitazioni all'esercizio da parte del soggetto segnalato. Il diritto alla Portabilità dei dati non risulta applicabile.
Rettifica (art. 16) e Diritto all'oblio (art.	Il segnalante può effettuare integrazioni e modifiche. Ai sensi dell'art. 22 del D.lgs. 24/2023, le rinunce e le transazioni, integrali o parziali, che hanno per oggetto i diritti e le tutele previsti dal decreto non sono

[1] I diritti previsti agli artt. 15-22 GDPR non possono essere esercitati né con richiesta al titolare del trattamento né con reclamo al Garante per la Protezione dei dati Personali, qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto 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.

17) e Obbligo di notifica (art. 19)	valide, salvo che siano effettuate nelle forme e nei modi di cui all'articolo 2113, quarto comma, del Codice civile. L'Obbligo di notifica non risulta applicabile. I diritti di rettifica, oblio e notifica non si applicano al soggetto segnalato.
Limitazione e opposizione trattamento (art. 18, 19 e 21) e reclami (artt. 41, 43, 57)	I diritti di limitazione e opposizione non si applicano al soggetto segnalato. In ogni caso è possibile proporre reclamo all'Autorità Garante sia da parte dei soggetti segnalanti che segnalati.
Rapporti con i Responsabili del trattamento (art. 28)	Nomina dei soggetti delegati nella veste di responsabile del trattamento di dati personali con istruzioni specifiche, con particolare riguardo alla necessità di conservazione in massima sicurezza. Audit periodici della piattaforma.
Garanzie riguardanti trattamenti internazionali (capo V)	Non sono previste esportazioni di dati fuori dalla UE (datacenter posizionato in Italia).
Consultazione preventiva (articolo 36)	Consultazione preventiva non effettuata in quanto il trattamento anche in ragione delle misure adottate dal titolare non presenta rischi elevati per i diritti e le libertà dell'interessato.
Gestione rischi per i diritti e le libertà degli interessati	
Impatto potenziale per i diritti e le libertà degli interessati	**ALTO**
Valutazione della probabilità	**MEDIO BASSA**
Livello di rischio rilevato	RISCHIO = IMPATTO (**ALTO**) X PROBABILITÀ (**MEDIO BASSA**) = **MEDIO**
Fonti di rischio (Accesso illegittimo, modifica indesiderata, scomparsa dei dati)	Valore dato dalla Riservatezza: **MEDIO** Valore dato dalla Integrità: **MEDIO** Valore dato dalla Disponibilità: **MEDIO** Valore dato dalla Resilienza: **MEDIO** Valore dato dalla Accountability: **MEDIO**
Risultanze complessive dell'Analisi del rischio	Livello di rischio complessivo: **MEDIO** (vedi Allegato 1 – Report analisi dei rischi piattaforma Whistleblowing)
Misure previste per gestire i rischi (art. 35, paragrafo 7, lettera d)	Vedi misure attive indicate nel documento analisi dei rischi. Attivi soltanto protocolli TLS 1.2 e 1.3 Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema è protetta con chiave asimmetrica personale e protocollo a curve ellittiche (*Cipher Negotiated* di tipo "TLS_AES_256_GCM_SHA384, 384 bit ECDH (P-384)") per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato è salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento.

	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. L'applicativo implementa un sistema di audit log sicuro e *privacy preserving* atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. Altri elementi di sicurezza implementati: • sistema progettato in conformità alla norma ISO 27001:2022; • crittografia completa dei dati delle segnalazioni degli informatori e delle comunicazioni dei destinatari; • supporto dell'anonimato digitale con l'integrazione di Tor; • supporto HTTPS integrato con lo standard TLS 1.3 (classificazione SSLabs A+); • registrazione automatica gratuita del certificato digitale (Let's Encrypt); • non sono state rilevate vulnerabilità tecniche di particolare gravità, comunque facilmente risolvibili; • test di penetrazione multipli con rapporti pubblici completi; • conformità agli standard di settore e alle best practice per la sicurezza delle applicazioni (OWASP); • il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238; • *sandboxing* di rete integrato con iptables; • *sandboxing* dell'applicazione integrato con AppArmor; • protezione completa contro gli invii automatici (prevenzione dello spam); • soggetto a continue revisioni tra pari e controlli di sicurezza periodici; • supporto PGP per notifiche e-mail crittografate e download di file crittografati; • non lascia tracce nella cache del browser. L'appuntamento presso l'ufficio del Responsabile della Prevenzione della Corruzione e della Trasparenza della **Provincia di Ancona** non è tracciato, né rispetto al momento, né rispetto al soggetto segnalante, ferme restando le successive necessarie attività di riconoscimento e verbalizzazione.
Implementazione (rapida) di un sottoinsieme di ulteriori/successive misure di sicurezza	
Elenco sistemi utilizzati nel trattamento	Sistema di virtualizzazione; Virtual machine isolata e dedicata alla sola piattaforma; Whistleblowing; Piattaforma per la gestione informatizzata della segnalazione.
Misure di sicurezza da adottare per attenuare il rischio	Migliorare le indicazioni ai soggetti segnalanti al fine di evitare di lasciare traccia in più dispositivi o sistemi: ad esempio utilizzare sistemi al di fuori della rete dell'Organizzazione, con navigazione anonima.
Misure di sicurezza consigliate per attenuale il rischio	Eliminare la vulnerabilità di livello medio riscontrata (CVSS: 5.9 - NVT: SSL/TLS: BREACH attack against HTTP compression).

Ulteriori misure di sicurezza per innalzare la maturità del sistema	Effettuare periodici Vulnerability assessment della piattaforma. Simulare segnalazioni al fine di verificarne la correttezza del processo.
Altre Info utili alla valutazione	N/A
Risultanze ricalcolo Analisi del rischio	Livello di rischio complessivo: Accettabile con riserva di adozione delle misure indicate.
Parere del DPO	Si rilascia parere positivo considerato l'obbligo di legge e la piattaforma utilizzata.
Indicazioni del DPO (art. 35, par. 2)	Accettate.
Opinioni interessati o loro rappresentanti (art. 35, par. 9)	Considerata la tipologia di servizio non si è ritenuto necessario richiedere parere agli interessati. Resta fermo l'ascolto di ogni istanza da parte dei loro rappresentanti.
Esito finale della valutazione	In funzione dell'analisi effettua il trattamento in oggetto ha un livello di rischio accettabile che non necessita di comunicazione all'Autorità Garante secondo quanto previsto dall'art. 36 GDPR "Consultazione preventiva". Si consiglia comunque di adottare dei controlli in itinere, con audit specifici, in modo da verificare che le attività di trattamento siano effettuate secondo indicazioni; è necessario registrare evidenze dell'audit e relative prescrizioni in caso di non conformità rilevate.
Note	Nessuna
Versioning DPIA	Versione 02 del 04/08/2023 redatta da: DPO e team.

.

Informativa “Segnalazione Condotte Illecite”

Articoli 13 -14 - Regolamento (UE) n. 2016/679 “GDPR”

Gentile Segnalatore,
con la presente informativa il Titolare (di seguito anche “Organizzazione”) intende informarLa sul trattamento dei Suoi dati personali necessari alla gestione delle segnalazioni delle condotte illecite previste dalla disciplina del D.lgs. 24/2023, ovvero l’istituto, recentemente revisionato nel nostro ordinamento, con il quale si assicura che colui (dipendente nonché collaboratore di impresa fornitrice dell’Amministrazione) che effettua, secondo certe modalità, nell’interesse dell’integrità della pubblica amministrazione, la segnalazione di condotte illecite o irregolarità di cui sia venuto a conoscenza in ragione del proprio rapporto di servizio, sia soggetto a particolari tutele. Si riportano di seguito le informazioni ai sensi degli artt. 13- 14 del Regolamento (UE) 2016/679 (di seguito anche “Regolamento”) sul trattamento dei dati personali dei soggetti che effettuano segnalazioni di illeciti ai sensi del D.lgs. 10 marzo 2023 n. 24 in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019.

TITOLARE DEL TRATTAMENTO:
Provincia di Ancona

RESPONSABILE PROTEZIONE DATI (RPD/DPO): dpo@morolabs.it

COSA FACCIAMO CON I SUOI DATI (Categorie dati, requisito necessario)
Il trattamento è una qualsiasi operazione effettuata sui dati personali come raccolta, organizzazione, conservazione, consultazione o interconnessione. In relazione alle finalità del trattamento possiamo ricevere da Lei soltanto i Suoi dati personali, sia di tipo “comune” come il Suo nome, cognome, data di nascita, dati di contatto o altri dati identificativi, sia di tipo potenzialmente “particolare”, come i contenuti della segnalazione. Il segnalante può comunicare qualsiasi tipologia di informazione (riferita tanto alle persone fisiche oggetto della segnalazione come a sé stesso) al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l’organizzazione, commesse dai soggetti che a vario titolo interagiscono con la medesima. Si invita il segnalante a comunicare le sole informazioni indispensabili.
Non è necessario riportare il proprio nominativo ma, al fine di ricevere comunicazioni e feedback dall’organizzazione, è necessario riportare un riferimento oppure conservare il codice della segnalazione in modo da ottenere i dovuti riscontri, conformemente alla vigente normativa.

PERCHÉ TRATTIAMO I SUOI DATI (Finalità, base giuridica)
Le basi giuridiche previste per la gestione delle segnalazioni di presunte condotte illecite sono le seguenti:
- art. 6 par. 1 lettera c) (“*il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento*”), qualora siano trattati dati personali diversi da quelli afferenti alle categorie particolari o a condanne penali e reati;
- art. 9 par. 2 lettera g) (“*trattamento è necessario per motivi di interesse pubblico rilevante*”), qualora siano trattati dati particolari;
- art. 10 (“*il trattamento dei dati personali relativi alle condanne penali o ai reati o a connesse misure di sicurezza, deve avvenire soltanto se il trattamento è autorizzato dal diritto dell’Unione o degli Stati Membri*”), qualora siano trattati dati relativi a condanne penali e reati;

Il suddetto trattamento dei dati avviene nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di acquisire gli elementi volti a consentire l’accertamento di eventuali illeciti denunciati nell’interesse dell’integrità dell’Amministrazione ai sensi del D.lgs. 24/2023.
I segnalanti hanno libera facoltà di decidere se inserire i propri dati identificativi o meno, senza che ciò limiti la possibilità di completare la segnalazione.

Informativa “Segnalazione Condotte Illecite”

Articoli 13 -14 - Regolamento (UE) n. 2016/679 “GDPR”

La liceità del trattamento è rinvenibile anche all’art. 13 del D.lgs. 24/2023 (Attuazione della direttiva (UE) 2019/1937, 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). Le segnalazioni saranno gestite dal Responsabile della prevenzione della corruzione e della trasparenza attraverso i canali o le piattaforme previste.

COME TRATTIAMO I SUOI DATI E CON QUALI MEZZI (Modalità di trattamento)
I dati saranno trattati con strumenti prevalentemente cartacei, nel rispetto delle misure di sicurezza tecnico organizzative previste dalla regolamentazione interna.

DOVE FINISCONO I SUOI DATI (Fonte dei dati, Comunicazione a terzi e categorie di destinatari)
I dati sono raccolti tramite il canale di segnalazione scritto previsto o tramite la segnalazione orale del segnalante e possono coinvolgere altre persone, quali Segnalati, Facilitatori o altri soggetti previsti dalla disciplina. Il destinatario principale dei dati è il Responsabile della prevenzione della corruzione e della trasparenza.
Sono destinatari dei dati raccolti a seguito della segnalazione, se del caso, l’Autorità Giudiziaria, la Corte dei conti e l’ANAC. I dati personali raccolti sono altresì trattati dal personale dell’organizzazione, che agisce sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento medesimo. Si fa presente, inoltre, che la segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della Legge 241/1990, dagli articoli 5 e seguenti del D.lgs. 33/2013 nonché dagli artt. 15-22 GDPR.
I dati non saranno oggetto di trattamento in paesi al fuori dell’Unione Europea, garantendo così i livelli di protezione previsti dalla vigente disciplina.

QUANTO TEMPO CONSERVIAMO I SUOI DATI (Periodo di conservazione)
Le segnalazioni 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. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

DA CHI RICEVIAMO I SUOI DATI (Fonte dei dati)
La fonte da cui hanno origine i dati personali è la segnalazione effettuata dal soggetto segnalante.

QUALI SONO I SUOI DIRITTI
I segnalanti hanno il diritto di richiedere e ottenere dall’organizzazione, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento), nei limiti previsti dall’art. 22 del D.lgs. 24/2023 (Rinunce e transazioni). In ogni caso, l’eventuale esercizio di altri diritti previsti dall’ordinamento europeo e nazionale (segnatamente l’accesso ai documenti amministrativi, l’accesso civico e l’accesso ai dati personali, cfr. art. 12, comma 8, del Decreto D.lgs. 24/2023, in riferimento agli artt. 22 e ss. della l. n. 241/1990 e all’art. 5 e ss. del d.lgs. 33/2013, nonché art. 13, comma 3, del Decreto, in riferimento agli artt. 15-22 del Regolamento e all’art. 2-undecies del Codice) è sottoposto a deroghe e limitazioni all’esercizio da parte del soggetto segnalato.

Informativa “Segnalazione Condotte Illecite”

Articoli 13 -14 - Regolamento (UE) n. 2016/679 “GDPR”

COME PUÒ ESERCITARE I SUOI DIRITTI

A volte l’evoluzione tecnologica non ci facilita il compito di proteggere i Suoi dati.
I segnalanti in caso di dubbi o di necessità potranno esercitare i loro diritti contattando il Titolare del trattamento oppure il Responsabile della protezione dei dati utilizzando il modulo di esercizio dei diritti presente sul sito web istituzione, area GDPR.
Altrimenti hanno il diritto di proporre un reclamo all’Autorità Garante per la Protezione dei Dati Personali (e-mail: protocollo@gpdp.it – www.garanteprivacy.it).

AGGIORNAMENTI

L’Informativa è lo strumento previsto dal Regolamento per applicare il principio di trasparenza e agevolare la gestione delle informazioni che trattiamo. Al variare delle modalità di trattamento, della normativa nazionale o europea, l’Informativa potrà essere revisionata ed integrata; in caso di cambiamenti importanti, sarà data notizia nella *home page* del sito web istituzionale.

.

Provincia di Ancona

CERTIFICATO DI IMMEDIATA ESEGUIBILITA'

DECRETO DEL PRESIDENTE DELLA PROVINCIA
N. 41 DEL 10/04/2025

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

Si certifica che il presente decreto è stato dichiarato immediatamente eseguibile (art. 21-quater della Legge n. 241/1990) il 10/04/2025.

Ancona, 14/04/2025

IL SEGRETARIO GENERALE

SAVINI MARINA

(sottoscritto digitalmente ai sensi dell'art. 21 D.Lgs. n. 82/2005 e s.m.i.)

.

Provincia
di Ancona

CERTIFICATO DI PUBBLICAZIONE

DECRETO DEL PRESIDENTE DELLA PROVINCIA
N. 41 DEL 10/04/2025

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

Si certifica che copia del presente decreto è affisso all'Albo pretorio on line per 15 giorni consecutivi dal 14/04/2025.

Ancona, 14/04/2025

IL RESPONSABILE

LAMPA LAURA

(sottoscritto digitalmente ai sensi
dell'art. 21 D.Lgs. n. 82/2005 e s.m.i.)

COPIA CONFORME ALL'ORIGINALE

Si attesta che la presente copia è conforme all'originale firmato digitalmente.

Il Responsabile

.

Provincia
di Ancona

CERTIFICATO DI ESECUTIVITA'

DECRETO DEL PRESIDENTE DELLA PROVINCIA
N. 41 DEL 10/04/2025

OGGETTO: PROCEDURA PER IL RICEVIMENTO E LA GESTIONE DELLE SEGNALAZIONI DI ILLECITO WHISTLEBLOWING, D. LGS. N. 24/2023 DI ATTUAZIONE DELLA DIRETTIVA (UE) 2019/1937. ADESIONE AL SERVIZIO WHISTLEBLOWING PA DI TRANSPARENCY INTERNATIONAL ITALIA E WHISTLEBLOWING SOLUTION IMPRESA SOCIALE

Su conforme attestazione del funzionario incaricato, si certifica che il presente decreto è divenuto esecutivo, ai sensi dell'art. 134, comma 3, del D.Lgs. n. 267/2000 il 11/04/2025

Ancona, 14/04/2025

IL SEGRETARIO GENERALE

SAVINI MARINA

(sottoscritto digitalmente ai sensi
dell'art. 21 D.Lgs. n. 82/2005 e s.m.i.)

.