Ditta:

Assiservizi XL S.a.s. di Da Rold Sebastiano

P.I. 01275360251

Sede

Via Garibaldi, 5

32032 Feltre (BL)

DATA PROTECTION IMPACT ASSESSMENT – D.P.I.A.

Gestione delle segnalazioni interne (c.d. whistleblowing)

Ai sensi dell'art. 13 comma 6 del D. Lgs. n. 24 del 10 marzo 2023 e
in conformità all'art. 35 del Regolamento UE 2016/679

Revisione Data	Paragrafo modificato	Descrizione della modifica	Origine della modifica
00 23/04/2024	-----	*Prima stesura*	-----

Il Legale rappresentante _____

INDICE

Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), la DPIA corrisponde alla valutazione d'impatto del trattamento del dato sulla protezione dei dati, qualora il trattamento possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Ciò considerata la natura, il contesto e le finalità del trattamento.

Il GDPR introduce dunque una valutazione di stampo preliminare, che consente al Titolare del trattamento di prendere visione del rischio prima ancora di procedere al trattamento, e di attivarsi perché tale rischio possa essere, se non annullato, quantomeno fortemente ridotto.

I principi fondamentali datenere in considerazione per l'esecuzione della DPIA risultano pertanto:

- i diritti e le libertà fondamentali dell'interessato, peraltro punto cardine dell'intero impianto del GDPR, i quali sono "non negoziabili", stabiliti dalla legge, obbligatoriamente rispettati e non soggetti ad alcuna variazione, indipendentemente dalla natura, gravità e probabilità dei rischi;
- la gestione dei rischi del trattamento, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio.

La metodologia di analisi dei rischi adottata nella conduzione della presenta Data Protection Impact Assessment è la metodologia di analisi della CNIL, Commission nationale de l'informatique et des libertés, Autorità Garante francese per la protezione dei dati personali.

1. Contesto

1.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni ai sensi del D. Lgs. n. 24/2023 (c.d. Decreto Whistleblowing), ma anche del segnalato e di tutti i soggetti eventualmente coinvolti nella segnalazione, e riguarda l'intero ciclo di vita della segnalazione.

Segnalazione in forma orale

La segnalazione effettuata oralmente, previo consenso del segnalante, sarà documentata a cura dell'Organo di valutazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto.

Segnalazione in forma scritta

La segnalazione va fatta utilizzando l'apposito modulo allegato alla procedura *Privacy completa* e reso disponibile nella bacheca utilizzata per le comunicazioni al personale presente presso ciascuna sede. La firma del segnalante sul modulo deve essere posta "a mano".
Il segnalante dovrà inviare la segnalazione presso la sede del Responsabile dei Sistemi Interni di Segnalazione delle Violazioni (RSISV).
Il segnalante avrà cura di predisporre due buste chiuse includendo, nella prima, i suoi dati identificativi unitamente a un documento d'identità e, nella seconda, l'oggetto della segnalazione. Entrambe le buste dovranno essere inserite in una terza busta nella quale dovrà essere riportata la dicitura "riservata al Responsabile dei Sistemi Interni di Segnalazione delle Violazioni (RSISV)"; al fine di garantire l'adeguata riservatezza, il segnalante NON DOVRÀ RIPORTARE NELLA TERZA BUSTA I PROPRI DATI DI MITTENTE.

1.1.1. Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	*Assiservizi XL Sas di Da Rold Sebastiano* (in seguito anche Titolare del trattamento) Via Garibaldi, 5 32032 Feltre (BL) P.I. 01275360251
Responsabile del trattamento	Responsabile dei Sistemi Interni di Segnalazione delle Violazioni (RSISV)
Sub Responsabile per _____	-----
Amministratore di Sistema	-----
Autorizzati al trattamento	-----

1.1.2. Standard applicabili al trattamento

- Regolamento UE n. 2016/679 (c.d. GDPR).
- D. Lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D. Lgs. n. 101/2018.
- Direttiva UE n. 2019/1937 del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione (c.d. Direttiva Whistleblowing).
- D. Lgs. n. 24/2023 "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. " (c.d. Decreto Whistleblowing).

Inoltre si segnala che il trattamento in questione non comporta alcun trattamento effettuato tramite sistemi decisionali o di monitoraggio automatizzati come previsto dal D. Lgs 104/2022; pertanto non si applica quanto previsto dal suddetto decreto.

1.2. Dati, processi (ciclo di vita) e risorse di supporto

Categorie dei dati trattati

- Dati identificativi (nome e cognome; possibili anche dati residenziali).
- Dati di contatto (email e telefono).
- Qualifica professionale e rapporto di servizio con il Titolare del trattamento.
- Dati relativi alle presunte condotte illecite segnalate, attribuite al segnalato, nelle quali l'interessato potrebbe essere coinvolto o delle quali potrebbe essere a conoscenza.
- Contenuti delle comunicazioni scambiate tra il segnalante e i soggetti che gestiscono la segnalazione.
- Immagini e altra documentazione eventualmente allegata alla segnalazione.
- Categorie particolari di dati personali eventualmente contenuti nella segnalazione.
- Dati giuridici eventualmente contenuti nella segnalazione.

Qualora, all'esito della verifica di una segnalazione di illecito si ravvisassero elementi di non manifesta infondatezza del fatto segnalato, al fine di attivare ulteriori approfondimenti istruttori o per l'adozione dei provvedimenti di competenza, potrebbero essere oggetto di trattamento una più ampia gamma di dati personali quali, a titolo esemplificativo e non esaustivo, posizione in organigramma, esperienze lavorative pregresse, titolo di studio, competenze professionali maturate, dati che rivelano l'origine razziale o etnica, dati che rivelano opinioni politiche, dati che rivelano l'appartenenza sindacale, dati che rivelano convinzioni religiose, dati relativi alla salute, dati relativi a condanne penali e reati, dati anagrafici dei familiari, ecc.

Soggetti interessati

- Il segnalante ovvero:

- lavoratori subordinati;
- candidati a posizioni lavorative vacanti, ove le informazioni sulle violazioni che intendono segnalare siano state acquisite durante il processo di selezione o in altre fasi precontrattuali;
- ex-dipendenti ovvero ex-collaboratori, ove le informazioni sulle violazioni che intendono segnalare siano state acquisite in costanza del rapporto di lavoro e/o di collaborazione;
- lavoratori autonomi, liberi professionisti e collaboratori;
- tirocinanti, retribuiti e non retribuiti;
- persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto.

– I soggetti segnalati indicati come presunti responsabili.
– I soggetti implicati nelle violazioni
– I soggetti al corrente dei fatti o comunque menzionati nella segnalazione.
– I facilitatori (se e quando previsti).

I dati personali dei soggetti diversi dal segnalante sono solitamente forniti dal segnalante tramite la segnalazione, oppure forniti dagli altri soggetti interessati qualora questi siano sentiti durante l'indagine.

1.2.1. Ciclo di vita del trattamento dei dati

Segnalazione in forma orale

La segnalazione effettuata oralmente, previo consenso del segnalante, sarà documentata a cura dell'Organo di valutazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto.

Tutta la documentazione prodotta andrà comunque cancellata al termine del tempo necessario per il trattamento della segnalazione, e comunque non oltre 5 anni a decorrere dalla data della comunicazione al segnalante dell'esito finale della procedura di segnalazione. Sono fatti salvi eventuali specifici obblighi normativi o la sopravvenuta necessità del Titolare del trattamento di agire o difendersi in giudizio, che rendano necessario il trattamento e la conservazione dei dati per periodi di tempo superiori.

Segnalazione in forma scritta

Il segnalante dovrà inviare la segnalazione presso la sede del Responsabile dei Sistemi Interni di Segnalazione delle Violazioni (RSISV).

Tutta la documentazione prodotta andrà comunque cancellata al termine del tempo necessario per il trattamento della segnalazione, e comunque non oltre 5 anni a decorrere dalla data della comunicazione al segnalante dell'esito finale della procedura di segnalazione. Sono fatti salvi eventuali specifici obblighi normativi o la sopravvenuta necessità del Titolare del trattamento di agire o difendersi in giudizio, che rendano necessario il trattamento e la conservazione dei dati per periodi di tempo superiori.

Le segnalazioni fuori campo di applicazione del D. Lgs. 24/2023 non saranno prese in considerazione, e pertanto per esse il ciclo di vita è limitato alla presa coscienza della loro non applicabilità.

1.2.2. Risorse di supporto ai dati

Segnalazione in forma orale

Le risorse di supporto ai dati sono:

- Device telefonico ad uso dei componenti dell'Organo di valutazione.
- Dispositivo idoneo alla conservazione e all'ascolto (se del caso).

Segnalazione in forma scritta

Le risorse di supporto ai dati sono:

- Cassettieria / anta di armadio con serratura e chiave.

2. Principi fondamentali

2.1. Proporzionalità e necessità

Finalità del trattamento

Il trattamento viene effettuato per le seguenti finalità:

- ricezione e gestione della segnalazione;
- istruttoria volta a verificare la fondatezza del fatto oggetto della segnalazione, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati;
- applicazione di misure correttive e/o di provvedimenti;
- monitoraggio della loro applicazione;
- aggiornamento del segnalante sulla presa in carico della segnalazione e sulla conclusione dell'istruttoria conseguentemente avviata;
- difesa in giudizio del Titolare del trattamento;
- difesa in giudizio del segnalante.

Basi giuridiche del trattamento

Le attività di trattamento sono svolte in base ad un obbligo legale a cui il Titolare del trattamento è soggetto (art. 6 par. 1 lett. c) - GDPR) nel rispetto della normativa di riferimento riguardante i soggetti che segnalano illeciti (*whistleblowing* - D. Lgs 24/2023).

Qualora, nell'ambito di una segnalazione, vengano fornite anche categorie particolari di dati personali, il Titolare del trattamento le tratterà in virtù delle seguenti deroghe:

- necessità di assolvere gli obblighi ed esercitare i diritti specifici del Titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (art. 9 par. 2 lett. b) - GDPR);
- necessità di accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (art. 9 par. 2 lett. f) - GDPR) per quanto concerne il trattamento dei dati personali necessari in sede di contenzioso o in sede precontenziosa, per far valere o difendere un diritto, anche del Titolare del trattamento o di un terzo, in sede giudiziaria, nonché in sede amministrativa o di arbitrato e conciliazione.

Per quanto concerne la rivelazione dell'identità del segnalante a soggetti diversi da quelli competenti a ricevere la segnalazione, e l'utilizzabilità della segnalazione se l'identità del segnalante è necessaria per la difesa del segnalato, in conformità a quanto previsto dall'art. 12 commi 2 e 5 del D. Lgs 24/2023, la base giuridica è rappresentata dal consenso.
Analogamente, il consenso del segnalante è necessario per la conservazione di eventuali registrazioni e/o trascrizioni di telefonate, messaggi, conversazioni (art. 14 commi 2 e 4 del D. Lgs 24/2023).

Minimizzazione dei dati

I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D. Lgs. n. 24/2023.
Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (art. 5.1. lett. c) GDPR).

I dati sono esatti e aggiornati

Il trattamento dei dati personali relativi alle segnalazioni sono costantemente aggiornati in quanto i soggetti autorizzati a ricevere e gestire le segnalazioni, i componenti dell'Organo di valutazione, ne verificano la corrispondenza a verità attraverso indagini mirate come previsto dalla procedura per la gestione delle segnalazioni.

Periodo di conservazione

I dati personali, la segnalazione e la relativa documentazione saranno conservati per il tempo necessario al trattamento della segnalazione, e comunque non oltre 5 anni a decorrere dalla data della comunicazione al segnalante dell'esito finale della procedura di segnalazione.

Sono fatti salvi eventuali specifici obblighi normativi o la sopravvenuta necessità del Titolare del trattamento di agire o difendersi in giudizio, che rendano necessario il trattamento e la conservazione dei dati per periodi di tempo superiori.

2.2. Misure a tutela dei diritti degli interessati

Informazioni agli interessati

Gli interessati sono informati attraverso:

- una procedura operativa appositamente predisposta (*Privacy completa*);
- una specifica informativa resa ai sensi degli artt. 13-14 GDPR (nell'informativa privacy consultabile nell'area segnalazioni del sito web https://www.snaservice.it/).

La procedura operativa e l'informativa vengono rese disponibili secondo le seguenti modalità:

- comunicazione interaziendale;
- nelle bacheca bacheca utilizzata per le comunicazioni al personale presente presso ciascuna sede.

Esiste comunque una procedura operativa per la gestione dei diritti degli interessati: *PP-08.00 - Esercizio dei diritti in materia di protezione dei dati personali.*

Consenso degli interessati

Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati altrattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6 par. 1. lett. c) - GDPR), come già dettagliato al precedente §2.1.

Per quanto concerne la rivelazione dell'identità del segnalante a soggetti diversi da quelli competenti a ricevere la segnalazione, e l'utilizzabilità della segnalazione se l'identità del segnalante è necessaria per la difesa del segnalato, in conformità a quanto previsto dall'art. 12 commi 2 e 5 del D. Lgs 24/2023, la base giuridica è rappresentata dal consenso.
Analogamente, il consenso del segnalante è necessario per la conservazione di eventuali registrazioni e/o trascrizioni di telefonate, messaggi, conversazioni (art. 14 commi 2 e 4 del D. Lgs 24/2023).
In tali circostanze, il consenso sarà raccolto mediante apposita modulistica, attualmente non ancora predisposta.

Esercizio dei diritti degli interessati

Gli interessati possono esercitare i diritti di cui agli articoli da 15 a 22 - GDPR rivolgendosi al Titolare del trattamento attraverso i contatti aperti con i mebri dell'Organo di valutazione, ovvero tramite procedura di reclamo al Garante per la protezione dei dati personali ai sensi dell'art. 77 – GDPR.

Il Titolare del trattamento segnala, tuttavia, che i diritti di cui agli articoli da 15 a 22 - GDPR non possono essere esercitati con richiesta al Titolare del trattamento ovvero con reclamo ai sensi dell'art. 77 – GDPR 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, così come previsto dalla normativa vigente (*whistleblowing* - D. Lgs 24/2023).

Obblighi dei Responsabili del trattamento

Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti o altri atti giuridici, così come specificato al precedente § 1.1.1.

Trasferimento dei dati al di fuori dello Spazio Economico Europeo

Per questa tipologia di trattamento non è previsto alcun un trasferimento di dati personali al di fuori dello Spazio Economico Europeo, così come specificato al precedente § 1.2.2.

3. Misure esistenti o pianificate

Sicurezza dei documenti cartacei

Politiche relative ai documenti cartacei contenenti dati personali utilizzati nell'ambito del trattamento. Tali politiche descrivono come i documenti sono stampati, archiviati, distrutti e condivisi.

Tutti i documenti cartacei vengono conservati dall'Organo di valutazione, che verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati; gli archivi sono inoltre chiusi a chiave e l'accesso è consentito soltanto all'Organo di valutazione.

Politica di tutela della privacy

Esistenza di un'organizzazione idonea a guidare e verificare la protezione dei dati personali all'interno della struttura (designazione di un DPO/RPD, creazione di un organo di monitoraggio, ecc.).

Il Titolare del trattamento adotta un Modello Organizzativo sulla protezione dei dati personali.

Gestione dei rischi

Esistenza di una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.).

L'analisi dei rischi viene condotta secondo metodologia proposta dalla CNIL, Commission nationale de l'informatique et des libertés, Autorità Garante francese per la protezione dei dati personali, come indicato nel successivo §5.1.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Esistenza di un'organizzazione operativa per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.).

Il Titolare del trattamento ha predisposto una specifica procedura mirata per la gestione del data breach, *PP-07.00 - Violazione dei dati personali*,in conformità a quanto prescritto dagli artt. 33-34 del GDPR.

Vigilanza sulla protezione dei dati

Esistenza di misure che consentano una visione globale e aggiornata dello stato di protezione dei dati e della conformità con il GDPR (verifica della conformità dei trattamenti, obiettivi e indicatori, responsabilità, ecc.).

La vigilanza viene svolta dal DPO.

4. Rischi

4.1. Metodologia

Il Titolare del trattamento si è dotato di un sistema di calcolo del rischio basato su parametri oggettivi, al fine di stabilire se esiste un rischio elevato per il trattamento specifico. L'oggettivazione del rischio passa pertanto attraverso un modello di creazione della probabilità e della gravità dell'evento in grado di rispecchiare il contesto in cui l'organizzazione opera. Sono state identificate griglie oggettive di calcolo delle probabilità e gravità con riguardo ai diritti e alle libertà dell'interessato.

Probabilità (P)	Significato	Criterio di scelta
4	Massima	Il verificarsi del danno dipende da condizioni direttamente connesse alla situazione. Il verificarsi del danno non provocherebbe alcuna reazione di stupore. Eventi simili sono già accaduti in Agenzia o in aziende dello stesso tipo.
3	Importante	Il verificarsi del danno dipende da condizioni non direttamente connesse alla situazione ma possibili. Il verificarsi del danno provocherebbe reazioni di moderato stupore. Eventi simili sono stati già riscontrati.
2	Limitata	Il verificarsi del danno dipende da condizioni impreviste. Il verificarsi del danno provocherebbe reazioni di grande stupore tra gli addetti. Eventi simili si sono verificati molto raramente.
1	Trascurabile	Il verificarsi del danno è subordinato a un concatenamento di eventi indipendenti tra loro. Il verificarsi del danno è creduto impossibile dagli addetti. Non è mai accaduto nulla di simile.

Gravità (G)	Significato	Descrizione generica degli impatti (diretti e indiretti)
4	Massima	I soggetti interessati possono incontrare conseguenze irreversibili.
3	Importante	I soggetti interessati possono incontrare conseguenze significative, e difficoltà nella loro risoluzione, ma comunque superabili.
2	Limitata	I soggetti interessati possono incontrare inconvenienti superabili.
1	Trascurabile	Gli interessati non saranno coinvolti o potrebbero incontrare alcuni lievi inconvenienti senz'altro superabili.

Matrice Rischi (Ri) = P x G					
		Probabilità			
		1 - Trascurabile	2 – Limitata	3 – Importante	4 – Massima
Gravità	1 - Trascurabile	1	2	3	4
	2 – Limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 – Massima	4	8	12	16

4.2. Analisi dei rischi

4.2.1. Accesso illegittimo – Perdita della riservatezza

GRAVITÀ (G): 3	Importante I soggetti interessati possono incontrare conseguenzesignificative e difficoltà nella loro risoluzione, ma comunque superabili come: diffusione indesiderata dei propri dati, consultazione dei propri da parte di personale non autorizzato, problematiche di natura giuslavoristica e contrattuale, discriminazioni lavorative.
PROBABILITÀ (P): 2	Limitata Il sistema di conservazione dei documenti cartacei (cassetto o anta di armadio con serratura e chiave, con chiave nella sola disponibilità del Gestore dei canali di segnalazione, e il controllo degli accessi fisici) rende poco probabile l'accesso ai dati ai fini della visione/consultazione se non ai soggetti autorizzati e quindi formati e competenti. Residua il rischio di errore umano o dolo.
FONTI DI RISCHIO	Fonti umane (es. dipendenti, collaboratori, soggetti esterni all'organizzazione del Titolare del trattamento, la cui condotta può essere accidentale o intenzionale).
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al §3 del presente documento.
CALCOLO DEL RISCHIO RESIDUO (Ri): 6	Rischio ponderato ("P" x "G")di "Livello 6".

4.2.2. Accesso illegittimo – Perdita dell'integrità

GRAVITÀ (G): 2	Limitata I soggetti interessati possono incontrare conseguenze limitate come: necessità di dover rettificare o inoltrare nuovamente la segnalazione.
PROBABILITÀ (P): 1	Trascurabile Il sistema di conservazione dei documenti cartacei (cassetto o anta di armadio con serratura e chiave, con chiave nella sola disponibilità del Gestore dei canali di segnalazione, e il controllo degli accessi fisici) rende poco probabile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti. Trattandosi poi di documentazione cartacea, la stessa modifica risulterebbe facilmente visibile. Residua il rischio di errore umano o dolo.
FONTI DI RISCHIO	Fonti umane (es. dipendenti, collaboratori, soggetti esterni all'organizzazione del Titolare del trattamento, la cuicondotta può essere accidentale o intenzionale).
MISURE	Le misure che contribuiscono a mitigare il rischio sono

	quelle descritte al §3 del presente documento.
CALCOLO DEL RISCHIO RESIDUO (Ri): 2	Rischio ponderato ("P" x "G")di "Livello 2"

4.2.3. Accesso illegittimo – Perdita della disponibilità

GRAVITÀ (G): 2	Limitata I soggetti interessati possono incontrare conseguenze limitate come: necessità di dover rettificare o inoltrare nuovamente la segnalazione
PROBABILITÀ (P): 2	Limitata Il sistema di conservazione dei documenti cartacei (cassetto o anta di armadio con serratura e chiave, con chiave nella sola disponibilità del Gestore dei canali di segnalazione, e il controllo degli accessi fisici) rende poco probabile l'accesso ai dati ai fini della sottrazione / distruzione se non ai soggetti autorizzati e quindi formati e competenti. Residua il rischio di errore umano o dolo.
FONTI DI RISCHIO	Fonti umane (es. dipendenti, collaboratori, soggetti esterni all'organizzazione del Titolare del trattamento, la cuicondotta può essere accidentale o intenzionale) Fonti non umane (es. eventi catastrofici)
MISURE	Le misure che contribuiscono a mitigare il rischio sono quelle descritte al §3 del presente documento.
CALCOLO DEL RISCHIO RESIDUO (Ri): 4	Rischio ponderato ("P" x "G")di "Livello 2".

5. Parere delle parti

5.1. Parere del DPO

Il DPO esprime il proprio parere favorevole alla DPIA a lui sottoposta con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo e congruenti con il modello organizzativo adottato dall'Agenzia.

Per maggiori ragguagli si veda il *Rapporto del DPO a seguito di DPIA nr. 2024/01 del 23/04/2024*, in allegato alla presente DPIA.

5.2. Parere degli interessati

Non è stato richiesto un parere agli interessati del trattamento in quanto appartenenti ad una generalità indistinta.

6. Conclusioni

Dall'analisi condotta nella presente DPIA, emergono rischi inerenti al trattamento con impatto sui diritti e le libertà degli interessati, stimati, al valore di "Livello 6", "Livello 4" e "Livello 2", per un valore medio di "Livello 4".

Con l'implementazione delle misure tecnico/organizzative sopra indicate (si veda il precedente §3), il valore di rischio rientra pertanto entro parametri di tolleranza.

Si ritiene in conclusione che il trattamento in oggetto non presenti rischi significativi per i diritti e le libertà dell'interessato e di conseguenza, non risulta richiesta la consultazione preventiva con l'Autorità Garante per la protezione dei dati personali, ex art. 36, par. 1 GDPR.