Data Privacy Impact Assessment (DPIA)
Whistleblowing – A.B.P. NOCIVELLI S.P.A

1. Premessa

Ai sensi dell'art. 13 comma 6 del d. lgs. 24/2023 i soggetti del settore privato, che sono tenuti all'attivazione di un canale di segnalazione interna, definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati. A mente dell'art. 35 del Regolamento UE n. 2016/679 (in seguito anche "GDPR"), tale valutazione è, del resto, obbligatoria ogniqualvolta il trattamento preveda l'uso di nuove tecnologie che, considerati la natura, l'oggetto, il contesto e le finalità, presenta un rischio elevato per i diritti e le libertà delle persone fisiche. Essa si sostanzia in una valutazione 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 annullato, o quantomeno fortemente ridotto.
La presente DPIA è effettuata, tenuto conto di quanto segue:

- i principi e i diritti fondamentali stabiliti dalla legge devono essere rispettati e tutelati;
- i rischi per la privacy dei soggetti interessati devono essere minimizzati mediante utilizzo di idonei strumenti tecnici di controllo e gestione.

2. Contesto

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali raccolti per effetto delle segnalazioni rese ai sensi del D.lgs. n. 24/2023. I dati degli interessati (segnalanti, segnalati ed eventuali altri soggetti terzi coinvolti) possono essere forniti dal medesimo soggetto interessato, oppure da terzi (è il caso, ad esempio, dei dati della persona segnalata, che sono forniti dal segnalante e dei dati acquisiti nell'ambito dell'attività istruttoria, svolta dal Responsabile della gestione del canale di segnalazione interno, cd. Responsabile Whistleblowing). La gestione delle segnalazioni viene effettuata attraverso la piattaforma adottata dalla Società, di cui vengono riportate le principali caratteristiche.

ARCHITETTURA DI SISTEMA	La piattaforma informatica di segnalazione è basata sul software TeamSystem Whistleblowing powered by GlobaLeaks. L'applicativo implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso

	al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. I datacenter del fornitore dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. Il fornitore di hosting è certificato ISO 9001:2015 e ISO 27001:2013.

In via residuale ed alternativa, le segnalazioni possono essere presentate mediante lettera in busta chiusa spedita a mezzo posta ordinaria alla sede della Società, in via Padana Superiore n. 67 - 25045 Castegnato (Brescia), posta all'attenzione dell'Organismo di Vigilanza; nonché mediante comunicazione, a mezzo posta elettronica, indirizzata al Responsabile Whistleblowing, all'indirizzo odv@abpnocivelli.com.

2.2 Responsabilità connesse al trattamento

Ruolo	**Nominativo**
Titolare del trattamento	A.B.P. NOCIVELLI S.P.A
Responsabile del trattamento	Team Systema Spa Sub-responsabili: Smart Flow Srl SB Synesthesia Srl SB Host.it
Incaricato al trattamento	Organismo di Vigilanza ex D.LGS 231/2001

2.3 Standard applicabili al trattamento

Al trattamento in materia di segnalazioni interne si applicano le seguenti normative:

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 1937/2019
D.lgs. n. 24/2023

2.4 Dati, processi e risorse di supporto

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione ai sensi del D.lgs. n. 24/2023:

Categoria di dato personale	**Categoria di interessato**
Dati personali comuni e di contatto	Dipendenti, collaboratori e lavoratori in genere, membri degli organi sociali, consulenti esterni, clienti e/o fornitori che effettuano una segnalazione o che vengono segnalati

Dati personali particolari (es. dati relativi alla salute, dati relativi all'appartenenza sindacale)	Dipendenti, collaboratori e lavoratori in genere, membri degli organi sociali, consulenti esterni, clienti e/o fornitori che effettuano una segnalazione o che vengono segnalati
Dati giudiziari (es. condanne penali)	Dipendenti, collaboratori e lavoratori in genere, membri degli organi sociali, consulenti esterni, clienti e/o fornitori che effettuano una segnalazione o che vengono segnalati

2.5 Ciclo di vita del trattamento dei dati

Mediante utilizzo della piattaforma

- Attivazione e configurazione della piattaforma;
- Utilizzo della piattaforma – invio delle segnalazioni da parte dei segnalanti ed accesso alle stesse da parte dei soggetti autorizzati;
- Dismissione della piattaforma (termini contrattuali o di legge) con conseguente cancellazione sicura dei dati da parte del fornitore/provider del servizio;

Mediante utilizzo di canali alternativi

- Raccolta della segnalazione;
- Attribuzione di uno specifico codice e protocollazione della stessa su un registro informatico, accessibile mediante credenziali, con indicazione del giorno e ora della segnalazione, del soggetto segnalante (se noto) e dell'oggetto della segnalazione;
- Archiviazione dei dati raccolti o acquisiti nell'ambito della fase istruttoria sul medesimo archivio digitale;
- Cancellazione dei dati quando non più necessari allo scopo ed in ogni caso entro 5 anni dalla comunicazione dell'esito finale della procedura di segnalazione.

2.6 Risorse a supporto dei dati

Piattaforma TeamSystem Whistleblowing.

3. Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi?	Il trattamento è finalizzato esclusivamente alla gestione della segnalazione ed all'adempimento degli obblighi derivanti dalla normativa vigente, in materia di cd. whistleblowing.
Quali sono le basi giuridiche che rendono lecito il trattamento?	Il trattamento è funzionale all'adempimento di un obbligo di legge (come previsto dal D. lgs. 24/2023) a cui è tenuto il Titolare (Art. 6.1. lett. c) GDPR).
I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?	I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come 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?	I dati personali relativi alle segnalazioni sono costantemente aggiornati, in quanto i soggetti incaricati di ricevere e gestire le segnalazioni ne verificano preliminarmente la corrispondenza a verità e li aggiornano, se necessario, nel corso dell'attività istruttoria.
Qual è il periodo di conservazione dei dati?	Le segnalazioni interne e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023.

3.1. Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?	Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità: - comunicazione indirizzata al personale in forza ed ai terzi sull'esistenza del canale di segnalazione interno (canale informatico); - pubblicazione sul sito internet della società, nella sezione dedicata al 'Whistleblowing';

	- affissione dell'informativa nei luoghi di lavoro.
Ove applicabile: come si ottiene il consenso degli interessati?	Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR). Ogniqualvolta invece sia richiesto il consenso del segnalante, quest'ultimo dovrà, tramite piattaforma, prestare il proprio consenso espresso alla comunicazione dei dati ai sensi degli artt. 6.1. lett. a) e 7 del GDPR.
Come fanno gli interessati a esercitare i loro diritti previsti dagli artt. 15 ss. GDPR?	Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR attraverso l'indirizzo di posta elettronica dedicato, nei limiti di cui all'articolo 2-undecies del Codice Privacy
Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?	La società TeamSystem Spa è Responsabile del trattamento ai sensi dell'art. 28 GDPR. Le Società Smart Flow Srl SB, Synesthesia Srl SB e Host.it (sono sub-responsabili). Tutte trattano i dati personali per conto del Titolare.
In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?	Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

4. Misure esistenti

Crittografia	In caso di utilizzo della piattaforma: L'applicativo implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing. Ogni informazione scambiata viene protetta in transito

	da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento. In caso di utilizzo di modalità alternative, i dati vengono protetti da apposite credenziali di accesso che impediscono l'accesso alla posta trasmessa ed al software di archiviazione digitale da parte di soggetti non autorizzati.
Controllo degli accessi logici	L'accesso applicativo alla piattaforma è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema supporta protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. In caso di utilizzo di modalità alternative, l'accesso alla posta trasmessa all'indirizzo odv@abpnocivelli.com ed al software di archiviazione digitale avviene tramite credenziali di autenticazione personali.
Tracciabilità	In caso di utilizzo della piattaforma: 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. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati. In caso di utilizzo di modalità alternative, le operazioni sono contraddistinte da un codice alfanumerico attribuito al momento della ricezione della segnalazione.

Archiviazione	L'applicativo implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura. I documenti ed i dati raccolti con modalità alternative, sono conservati nell'archivio digitale e cancellati irreversibilmente quando non più utili per lo scopo ed in ogni caso entro 5 anni dalla comunicazione dell'esito della procedura di segnalazione.
Gestione delle vulnerabilità tecniche	Globaleaks è periodicamente soggetto ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Quanto all'archivio digitale, viene adottata ogni cautela idonea a prevenire eventuali vulnerabilità e vengono eseguiti periodici controlli, funzionali a verificare l'esistenza di eventuali criticità.
Backup	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.
Manutenzione	È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing e per quelli che compongono l'infrastruttura fisica e di backup è prevista una modalità di manutenzione accessibile al personale TeamSystem e ai relativi fornitori, Smart Flow e Synesthesia, attraverso cui svolgere le modifiche al sistema e installare gli aggiornamenti.
Sicurezza dei canali informatici	Tutte le connessioni sono protette tramite protocollo TLS 1.2+ e connessioni con protocollo SSH.

Sicurezza dell'hardware	I datacenter del fornitore dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. Il fornitore di hosting è certificato ISO 9001:2015 e ISO 27001:2013.
Politica di tutela della privacy	Il Software adotta una politica di protezione dei dati personali conforme al GDPR ed al Codice della Privacy, applicando misure idonee a proteggerli da accessi non autorizzati, modifiche, danni e distruzione.
Vigilanza sulla protezione dei dati	La Vigilanza è svolta dal DPO

RIEPILOGO DELLE MISURA DI SICUREZZA FISICHE ADOTTATE

- Credenziali di autenticazione, assegnate individualmente ad ogni addetto.
  - Autenticazione mediante user-id e password.
  - Parola chiave di almeno 12 caratteri.
  - Disattivazione delle vecchie credenziali.
  - Disposizioni scritte per la disponibilità dei dati.
- Cifratura dei dati memorizzati.
- Cifratura dei dati trasmessi.
  - Cifratura con protocollo PGP.
- Sospensione automatica delle sessioni di lavoro.
- Sospensione manuale delle sessioni di Lavoro.
- Sono stati adottati adeguati criteri tra cui l'eventuale nomina a Responsabile per garantire che la struttura esterna presso cui l'unità di archiviazione risiede abbia adeguate contromisure che garantiscano un rischio residuale basso.
- Verifica e registrazione degli accessi dell'amministratore di sistema se questo è nominato direttamente dall'Azienda
- Verifica ed eventuale nomina degli amministratori di sistema se presenti
- Pseudonimizzazione.
- Trattamento dei dati con protocolli criptati.
- Profili di autorizzazione di ambito diverso per diversi incaricati.
  - È utilizzato un sistema di autorizzazione.
  - I profili di autorizzazione vengono specificati prima di ogni trattamento.
  - Verifica periodica del profilo di autorizzazione.

5. Rischi

5.1 Metodologia

Il livello di impatto è sempre correlato alle conseguenze che una violazione della sicurezza dei dati personali potrebbe avere per gli interessati, i cui dati sono stati violati.

Vengono presi in considerazione quattro livelli di impatto:

Livello di impatto	Descrizione
Basso	Gli individui possono andare incontro a piccoli disagi, superabili senza particolari problemi (ad es., il dover perdere un po' più di tempo per reinserire le informazioni…)
Medio	Gli individui possono andare incontro a disagi significativi, superabili ma con qualche difficoltà (ad es., il dover affrontare costi aggiuntivi, problemi ad accedere a servizi aziendali…)
Alto	Gli individui possono andare incontro a conseguenze significative, che probabilmente sapranno superare ma con grande difficoltà (ad es., in caso di appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà…)
Molto Alto	Gli individui possono andare incontro a conseguenze significative, o addirittura irreversibili, che potrebbero non essere in grado di superare (ad es. trovarsi nell'incapacità di lavorare…)

La valutazione dell'impatto è eseguita, tenendo conto delle specificità dell'operazione di trattamento.

I parametri considerati sono:

- la tipologia dei dati trattati: certi dati, se violati, possono impattare più di altri sull'individuo (ad es., dati sanitari, di appartenenza politica, di residenza o finanziari);
- il volume di dati trattati, sia dal punto di vista della quantità che dal punto di vista della durata temporale;
- le caratteristiche peculiari del Titolare del trattamento e degli interessati;

Nella valutazione dell'impatto sono considerati anche i possibili effetti collaterali secondari (sui diritti e le libertà delle persone).

La valutazione che segue permette di ottenere i diversi livelli di impatto per ciascuna delle seguenti tipologie di violazioni: perdita di riservatezza, perdita di integrità e perdita di disponibilità:

	Tipologia di violazione	Livello di gravità
1	PERDITA DI RISERVATEZZA Valutare l'impatto che una divulgazione non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	Basso Medio x Alto Molto Alto
2	PERDITA DI INTEGRITA' Valutare l'impatto che un'alterazione non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	Basso Medio x Alto Molto Alto
3	PERDITA DI DISPONIBILITA' Valutare l'impatto che una distruzione o perdita non autorizzata dei dati personali – nel contesto in cui il Titolare del trattamento svolge la propria attività – potrebbe avere sull'individuo	Basso x Medio Alto Molto Alto

5.2 Definizione delle possibili minacce

In questa sezione sono identificate le minacce correlate al contesto complessivo del trattamento dei dati personali e valutate la loro probabilità di accadimento.

Queste le quattro diverse aree di valutazione che interessano gli ambienti di elaborazione e trattamento dei dati, ovvero:

A) Risorse di rete e tecniche (hardware e software);

B) Processi / procedure relativi all'operazione di trattamento dei dati;

C) Parti e persone coinvolte nell'operazione di trattamento;

D) Settore di operatività e scala del trattamento.

A) Risorse di Rete e Tecniche

A. RISORSE DI RETE E TECNICHE		
1	Qualche parte del trattamento dei dati personali viene effettuata tramite Internet?	**SI** ~~NO~~

2	È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad esempio per determinati utenti o gruppi di utenti)?	~~SI~~ **NO**
3	Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno (alla tua organizzazione)?	**SI** ~~NO~~
4	Le persone non autorizzate possono accedere facilmente all'ambiente di trattamento dei dati?	~~SI~~ **NO**
5	Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le migliori prassi?	~~SI~~ **NO**

A. Le risposte nell'area sono:	Il livello di probabilità è:
Tutte negative o 1 sola positiva	☐ Basso
Due o tre risposte positive	X Medio
Tutte positive o 1 sola negativa	☐ Alto

B) Processi/Procedure relative all'operazione di trattamento

B. PROCESSI/PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO		
1	I ruoli e le responsabilità relativi al trattamento dei dati personali sono vaghi o non chiaramente definiti?	~~SI~~ **NO**
2.	L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non chiaramente definito?	~~SI~~ **NO**
3	I dipendenti sono autorizzati a portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?	~~SI~~ **NO**
4	I dipendenti sono autorizzati a trasferire, archiviare o altrimenti trattare dati personali al di fuori dei locali dell'organizzazione?	~~SI~~ **NO**
5	Le attività di elaborazione dei dati personali possono essere eseguite senza la creazione di file log di registro?	**SI** ~~NO~~

B. Le risposte nell'area sono:	Il livello di probabilità è:
Tutte negative o 1 sola positiva	X Basso
Due o tre risposte positive	☐ Medio
Tutte positive o 1 sola negativa	☐ Alto

C) Parti/Persone coinvolte nel trattamento dei dati personali

C. PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI		
1.	Il trattamento dei dati personali è eseguito da un numero non definito di dipendenti?	~~SI~~ **NO**
2.	Qualche parte dell'operazione di trattamento dei dati è eseguita da un appaltatore / terza parte (Responsabile del trattamento)?	**SI** ~~NO~~
3.	Gli obblighi delle parti / persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente definiti?	~~SI~~ **NO**
4.	Il personale coinvolto nel trattamento di dati personali non ha familiarità con le questioni di sicurezza delle informazioni?	~~SI~~ **NO**
5.	Le persone / le parti coinvolte nell'operazione di trattamento dei dati trascurano di archiviare e / o distruggere in modo sicuro i dati personali?	~~SI~~ **NO**

C. Le risposte nell'area sono:	Il livello di probabilità è:
Tutte negative o 1 sola positiva	X Basso
Due o tre risposte positive	☐ Medio
Tutte positive o 1 sola negativa	☐ Alto

D) Settore di operatività e Scala di trattamento

D. SETTORE DI BUSINESS E SCALA DI TRATTAMENTO		
1.	Ritieni che il tuo settore di operatività sia esposto agli attacchi informatici?	**SI** ~~NO~~
2.	La tua organizzazione ha subito attacchi informatici o altri tipi di violazioni della sicurezza negli ultimi due anni?	~~SI~~ **NO**
3.	Hai ricevuto notifiche e / o reclami riguardo alla sicurezza del tuo sistema informatico (utilizzato per il trattamento di dati personali) nell'ultimo anno?	~~SI~~ **NO**
4.	Un'operazione di elaborazione riguarda un grande volume di individui e/o di dati personali?	~~SI~~ **NO**
5.	Esistono *best practices* di sicurezza specifiche per il tuo settore di operatività che non sono state adeguatamente messe in atto?	~~SI~~ **NO**

D. Le risposte nell'area sono:	Il livello di probabilità è:
Tutte negative o 1 sola positiva	X Basso

Due o tre risposte positive	☐ Medio
Tutte positive o 1 sola negativa	☐ Alto

5.3 Valutazione delle probabilità di occorrenza delle minacce per area:

AREA DI VALUTAZIONE	PROBABILITÀ	
	LIVELLO	PUNTEGGIO
A. RISORSE DI RETE E TECNICHE	☐ Basso	1
	X Medio	2
	☐ Alto	3
B. PROCESSI/PROCEDURE RELATIVI ALL'OPERAZIONE DI TRATTAMENTO	X Basso	1
	☐ Medio	2
	☐ Alto	3
C. PARTI/PERSONE COINVOLTE NEL TRATTAMENTO DEI DATI PERSONALI	X Basso	1
	☐ Medio	2
	☐ Alto	3
D. SETTORE DI OPERATIVITA' E SCALA DI TRATTAMENTO	X Basso	1
	☐ Medio	2
	☐ Alto	3

5.4 Valutazione complessiva della minaccia:

SOMMA DEI PUNTEGGI DELLEQUATTRO AREE DI VALUTAZIONE	LIVELLO DI PROBABILITÀ DEL VERIFICARSI DELLA MINACCIA
4-5	Basso
6-8	Medio
9-12	Alto

5.5 Valutazione del rischio:

X RISCHIO BASSO

¨ RISCHIO MEDIO

¨ RISCHIO ALTO

5.7 Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento è l'adempimento di obblighi di legge. Prima dell'attivazione del canale di segnalazione interna, la società informerà le rappresentanze o le organizzazioni sindacali.

5.8 Parere DPO

Il DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conforme al dettato normativo.

6 Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono rischi di impatto sui diritti e libertà degli interessati con stima a valore **basso**, ritenuto accettabile dall'organizzazione in relazione ai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenti un grado di rischio sui diritti e libertà dell'interessato rientrante nei parametri accettabili e di conseguenza ***non è richiesta una consultazione preventiva all'Autorità Garante.***

Si allegano: valutazione di impatto fornita dal fornitore della piattaforma e nomina di Team System come responsabile del trattamento.

ELENCO DELLE REVISIONI

REV.	DATA	NATURA DELLE MODIFICHE	APPROVAZIONE
01	15/12/2023	Prima Emissione	CDA Titolare del trattamento