**VALUTAZIONE DI IMPATTO (DPIA)**

**Nome della DPIA:**

Valutazione d’impatto della procedura di *Whistleblowing.*

**TITOLARE DEL TRATTAMENTO:**

Azienda Speciale Riviere di Liguria, con sede legale e amministrativa: Via Quarda Superiore 16
17100 Savona

**Nome autore:**

Presidente CDA

Marina Meneghello (RPCT)

Gian Luca Ballero Dalla Dea (DPO)

**Nome Valutatore:**

Marina Meneghello (RPCT)

Gian Luca Ballero Dalla Dea (DPO)

**Validatore:**

Gian Luca Ballero Dalla Dea (DPO)

|  |  |  |
| --- | --- | --- |
| Data | Responsabili | Firma |
|  | TITOLARE |  |
|  | RPCT |  |
|  | ODV |  |
|  | Consulente Privacy |  |

INDICE

[1. DESCRIZIONE DEL TRATTAMENTO. 3](#_Toc152089941)

[1.1. Natura, ambito, contesto. 3](#_Toc152089942)

[1.1.1. Diritti della Carta dei Diritti Fondamentali dell'Unione europea da tutelare nell’ambito del trattamento in oggetto. 6](#_Toc152089943)

[1.1.2. Normativa e documenti aziendali di riferimento: 6](#_Toc152089944)

[1.1.3. Quale è il trattamento in considerazione? 7](#_Toc152089945)

[1.1.4. Finalità. 7](#_Toc152089946)

[1.2. Dati personali, destinatari e periodo di conservazione. 7](#_Toc152089947)

[1.2.1. I dati trattati. 7](#_Toc152089948)

[1.2.2. Interessati. 8](#_Toc152089949)

[1.2.3. Responsabile del trattamento. 8](#_Toc152089950)

[1.2.4. Sub-Responsabili del trattamento. 8](#_Toc152089951)

[1.2.5. Conservazione. 9](#_Toc152089952)

[1.3. Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)? 9](#_Toc152089953)

[1.4. Risorse. 9](#_Toc152089954)

[1.4.1. Quali sono le risorse di supporto ai dati? 9](#_Toc152089955)

[1.4.2. Persone che possono accedervi. 9](#_Toc152089956)

[2. NECESSITA’ E PROPORZIONALITA’. 10](#_Toc152089957)

[2.1. Misure previste per garantire il rispetto del GDPR. 10](#_Toc152089958)

[2.1.1. Piano di revisione della DPIA. 10](#_Toc152089959)

[2.1.2. Applicazione della Privacy by design, principi/strategie. 11](#_Toc152089960)

[2.1.3. Principi Fondamentali. 11](#_Toc152089961)

[2.1.4. Misure esistenti o pianificate. Politica di tutela della privacy. 11](#_Toc152089962)

[2.1.5. Controllo degli accessi fisico e logico. 11](#_Toc152089963)

[2.2. Misure che contribuiscono alla proporzionalità e alla necessità. Tracciabilità richieste di accesso. 12](#_Toc152089964)

[2.3. Finalità determinate, esplicite e legittime. 12](#_Toc152089965)

[2.4. Liceità del trattamento. 13](#_Toc152089966)

[2.5. I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)? 13](#_Toc152089967)

[2.6. Limitazione della conservazione. 13](#_Toc152089968)

[2.7. Misure a tutela dei diritti degli interessati. 14](#_Toc152089969)

[2.7.1. Come sono informati del trattamento gli interessati? 14](#_Toc152089970)

[2.7.2. Come fanno gli interessati a esercitare i loro diritti di cui agli articoli da 15 a 22 GDPR? 14](#_Toc152089971)

[3. RISCHI PER I DIRITTI E LE LIBERTA’ DEGLI INTERESSATI. 15](#_Toc152089972)

[3.1. Rischi. Individuazione della metrica del rischio. 15](#_Toc152089973)

[3.1.1. Le fonti di rischio: 16](#_Toc152089974)

[3.1.2. Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare? 16](#_Toc152089975)

[3.1.3. Principali minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati. 18](#_Toc152089976)

[3.1.4 Stime della probabilità e della gravità. 18](#_Toc152089977)

[3.2. Misure previste per gestire i rischi. 19](#_Toc152089978)

[4. OPINIONE DELLE PARTI INTERESSATE. 19](#_Toc152089979)

[4.1. Parere 19](#_Toc152089980)

[4.2. Conclusioni 20](#_Toc152089981)

# 1. DESCRIZIONE DEL TRATTAMENTO.

## 1.1. Natura, ambito, contesto.

Le informazioni e i dati personali sono forniti dal segnalante, nell’ambito delle procedure riguardanti le segnalazioni cd. *whistleblowing*, tramite il canale interno, aventi ad oggetto le “violazioni” come definite dalla procedura whistleblowing in vigore.

Le segnalazioni potranno essere effettuate:

1. in forma scritta con modalità informatiche crittografata, tramite la piattaforma whistlewblowingPA;
2. in forma orale, attraverso linee telefoniche ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole con l’RPCT di AZIENDA SPECIALE RIVIERE DI LIGURIA e/o con OdV.

Per quanto sopra le segnalazioni vengono acquisite, inizialmente, tramite tre canali:

1. con persona dedicata: RPCT, il quale ne potrà condividere i contenuti con OdV, ove la segnalazione riguardi materia di sua competenza (congiuntamente, nel prosieguo, il “**Gestore Segnalazione**”)

2. tramite un soggetto esterno con competenze specifiche **Whistleblowing solution IS S.r.l**

3. tramite canale della divulgazione pubblica (tramite stampa o social media).

In pratica, il soggetto Segnalante segnala al Responsabile della prevenzione della corruzione e della trasparenza (nel proseguo anche “**RPCT**”), destinatario della segnalazione, il quale deve:

1. curare l’istruttoria, se del caso con il supporto di OdV, rispettando la tutela della riservatezza e il principio di imparzialità nell’interesse generale e di tutte le parti coinvolte;
2. valutare i fatti;
3. chiedere chiarimenti (se strettamente necessari), inclusa l’audizione del segnalante e di eventuali altri soggetti;
4. utilizzare il contenuto delle segnalazioni per identificare le aree critiche dell’amministrazione in un’ottica di miglioramento della qualità ed efficacia del sistema di prevenzione della corruzione.

In caso di manifesta ed evidente infondatezza, RPCT può decidere di archiviare la segnalazione ovvero di:

a) predisporre gli interventi organizzativi necessari per rafforzare le misure di prevenzione della corruzione nell’ambito in cui è emerso il fatto segnalato;

b) inoltrare soltanto il contenuto della segnalazione, evidenziando che si tratta di una segnalazione su cui c’è una rafforzata tutela della riservatezza, a soggetti terzi interni competenti per l’adozione di eventuali ovvero a soggetti terzi esterni, se rileva la loro competenza (Autorità giudiziaria, Corte dei conti, ANAC).

Le segnalazioni rappresentano un efficace strumento diffuso di controllo ed emersione di ipotesi di corruzione e/o di mala gestio, nonché di eventuali violazioni del Modello 231/01. Tuttavia, per incoraggiare tali denunce, è necessario che colui che segnala l’illecito sia “protetto” da eventuali ritorsioni, anche nell’ambito lavorativo in cui offre la sua prestazione.

La segnalazione deve, poi, contenere elementi utili per consentire al RPCT di fare le verifiche e gli accertamenti del caso, oltre che di valutare la fondatezza, o meno, dei fatti segnalati.

Come chiarito dalla stessa ANAC, i contenuti minimi della segnalazione sono:

1. i dati del segnalante;
2. il luogo/struttura di lavoro e il periodo, anche indicativo, in cui si è verificato il fatto;
3. la chiara descrizione del fatto.

La segnalazione deve altresì contenere ogni altra informazione conosciuta o documento che possa confermare la fondatezza dei fatti segnalati. Non è necessario, invece, che il segnalantesia certo dell’effettivo verificarsi dei fatti denunciati o dell’autore, essendo sufficiente a tal fine che questi si sia prefigurato un’elevata probabilità che si verificasse il fatto. In ogni caso, non possono essere considerate meritevoli di tutela le segnalazioni fondate su meri sospetti o voci.

Le segnalazioni da cui non è possibile ricavare l’identità del segnalante sono considerate anonime.

Come noto le segnalazioni anonime, ove circostanziate, sono equiparate a segnalazioni ordinarie. I soggetti del settore pubblico che ricevono le segnalazioni tramite canali interni considerano le segnalazioni anonime alla stregua di segnalazioni ordinarie.

In ogni caso, il segnalante o il denunciante anonimo, successivamente identificato, che ha comunicato ad ANAC di aver subito ritorsioni può beneficiare della tutela che il decreto garantisce a fronte di misure ritorsive. AZIENDA SPECIALE RIVIERE DI LIGURIA, ove riceva segnalazioni attraverso il canale interno di segnalazione è tenuta a registrare le segnalazioni anonime ricevute e conservare la relativa documentazione non oltre cinque anni decorrenti dalla data di ricezione di tali segnalazioni, rendendo così possibile rintracciarle, nel caso in cui il segnalante, o chi abbia sporto denuncia, comunichi ad ANAC di aver subito misure ritorsive a causa di quella segnalazione o denuncia anonima.

Il quadro normativo in materia è teso all’adozione di specifiche misure per tutelare il dipendente segnalante. In particolare, si prevede che il segnalantenon possa essere sanzionato, demansionato, licenziato, trasferito o sottoposto ad altra misura organizzativa avente effetti negativi (diretti od indiretti) sulle condizioni di lavoro, in conseguenza della propria segnalazione, a pena di nullità dell’atto discriminatorio o ritorsivo. Al fine di attivare tale tutela, eventuali misure ritorsive adottate dal datore di lavoro devono essere comunicate all’ANAC dallo stesso interessato.

Il Titolare e il RPCT devono tener conto di questi rischi nella predisposizione dei mezzi di trattamento e nei loro comportamenti.

RPCT dovrà prestare particolare attenzione ad utilizzare esclusivamente gli strumenti dedicati alla gestione delle segnalazioni e a non utilizzare altri strumenti per i quali le tutele di riservatezza del segnalante potrebbero essere inferiori.

### 1.1.1. Diritti della Carta dei Diritti Fondamentali dell'Unione europea da tutelare nell’ambito del trattamento in oggetto.

* Art. 7. Rispetto della vita privata e familiare
* Art. 8. Protezione dei dati personali
* Art. 16 Libertà d’impresa
* Art. 21. Non discriminazione
* Art. 30 Tutela in caso di licenziamento ingiustificato
* Art. 41 Diritto ad una buona amministrazione

### 1.1.2. Normativa e documenti aziendali di riferimento:

* D.lgs. 231/2001 “Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300”, in particolare articolo 6 (abrogato);
* L. 190/2012 “Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione”;
* L. 179/2017 “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”;
* Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 “relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)” e Modello Privacy adottato da AZIENDA SPECIALE RIVIERE DI LIGURIA;
* D.Lgs. 196/2003 “Codice in materia di protezione dei dati personali ((, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE))”, come modificato dal D.lgs. 101/2018;
* Garante per la protezione dei dati personali, *Parere sullo schema di “Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell’art. 54-bis del D.Lgs. 165/2001 (c.d. whistleblowing)” - Registro dei provvedimenti n. 215 del 4 dicembre 2019;*
* Garante per la protezione dei dati personali, *Parere su uno schema di decreto legislativo recante attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell’Unione (cd. direttiva whistleblowing) - 11 gennaio 2023 [9844945];*
* D.Lgs. 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*”;
* Autorità Nazionale Anticorruzione, *Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell’Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne, Delibera n.311 del 12/7/2023,pibblicate in G.U.il 27/7/2023*;
* Linee Guida Anac approvate con delibera 311/2023.

### 1.1.3. Quale è il trattamento in considerazione?

Segnalazione di condotte illecite (*whistleblowing*) nell’ambito di appilcazione soggettivo ed oggettivo del D.Lgs. n 24/23.

### 1.1.4. Finalità.

La finalità consiste nel raccogliere le segnalazioni al fine di migliorare il sistema di prevenzione della corruzione al fine, in particolare, di favorire l'emersione di comportamenti atti od omissioni che ledono l’interesse pubblico o l’integrità di AZIENDA SPECIALE RIVIERE DI LIGURIA e che consistono in illeciti amministrativi, contabili civili, o penali, nonché le condotte illecite rilevanti ai sensi del decreto legislativo 8 giugno 2001, n, 231 o violazioni dei modelli di organizzazione e gestione ivi previsti.

Ai fini di incentivare le segnalazioni è fondamentale garantire la riservatezza dell’identità del segnalante (anche cd. “*whistleblower*”) e l’iter procedurale successivo alla segnalazione (riservatezza delle persone coinvolte e menzionate nella segnalazione, nonché del contenuto della stessa).

## 1.2. Dati personali, destinatari e periodo di conservazione.

### 1.2.1. I dati trattati.

I dati trattati riguardano informazioni e dati personali - di tipo comune, sensibile/particolare e giudiziario - forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio o altro rapporto giuridico con il Titolare, commesse dai soggetti che a vario titolo interagiscono con il medesimo.

Nello specifico si tratta di:

(•) Dati di identificazione personale, (•) dati relativi al ruolo ricoperto e inquadramento contrattuale, (•) dati relativi ad incarichi politici o incarichi di vertice nella PA, (•) dati giudiziari, (•) dati idonei a rivelare adesioni a partiti politici, sindacati, associazioni o organizzazioni a carattere religioso, filosofico, politico o sindacale, (•) categorie particolari di dati personali; (•) sottoscrizione del verbale redatto in caso di segnalazione effettuata con modalità orale; (•) tutti gli elementi della segnalazione dai quali si possa ricavare, anche indirettamente, l’identificazione del segnalante.

### 1.2.2. Interessati.

Persona segnalante o denunciate, facilitatore, persona coinvolta o persona menzionata nella segnalazione quali:

* dipendenti e i collaboratori, ivi inclusi i tirocinanti, di AZIENDA SPECIALE RIVIERE DI LIGURIA;
* alle persone del medesimo contesto lavorativo della persona segnalante, di colui che ha sporto una denuncia all'autorità giudiziaria o contabile o di colui che ha effettuato una divulgazione pubblica e che sono legate ad essi da uno stabile legame affettivo o di parentela entro il quarto grado
* ai colleghi di lavoro della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o effettuato una divulgazione pubblica, che lavorano nel medesimo contesto lavorativo della stessa e che hanno con detta persona un rapporto abituale e corrente
* agli enti di proprietà della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile o che ha effettuato una divulgazione pubblica o per i quali le stesse persone lavorano, nonché agli enti che operano nel medesimo contesto lavorativo delle predette persone
* gli azionisti e le persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza di AZIENDA SPECIALE RIVIERE DI LIGURIA;
* i liberi professionisti, i collaboratori e i consulenti che prestano la loro attività in favore di AZIENDA SPECIALE RIVIERE DI LIGURIA;
* i Fornitori/Clienti di AZIENDA SPECIALE RIVIERE DI LIGURIA.

### 1.2.3. Responsabile del trattamento.

WHISTLEBLOWING Solution S.r.l I.S., con sede legale in via Aretusa 34, 20129 Milano.

AZIENDA SPECIALE RIVIERE DI LIGURIA, Titolare del trattamento, ha dedicato particolare attenzione al funzionamento della piattaforma informatica destinata a gestire le segnalazioni. La piattaforma è stata individuata tra quelle elencate nei servizi SaaS di ACN e tra quest’ultime quelle che hanno conseguito le rilevanti certificazioni ISO. Quest’ultima agisce quale responsabile del trattamento, in base all’art. 28, paragrafo 1, del GDPR presenta “*garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell’interessato*”.

### 1.2.4. Sub-Responsabili del trattamento.

SEEWEB S.r.l

Il Titolare ha verificato che nessuno tra i Responsabili/Sub Responsabili effettua trasferimento dei dati personali al di fuori dello SEE anche concedendo l’accesso a tali dati a persone collocate al di fuori dello SEE.

### 1.2.5. Conservazione.

I dati personali raccolti per tale finalità verranno conservati per il tempo necessario alla loro definizione e, comunque, per non più di cinque anni a decorrere dalla data della comunicazione dell’esito finale della procedura di segnalazione. E’ stato appurato che sulla piattaforma WhistleblowingPA i dati vengono conservati per il periodo di mesi 24.

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

I dati vengono raccolti e trattati dal RPCT:

1. attraverso l’applicativo WHISTLEBLOWING Solution;
2. attraverso incontro fissato da RPCT su richiesta del segnalante.

La documentazione viene conservata in apposite cartelle di rete crittografate e, ove il canale utilizzato sia l’applicativo WHISTLEBLOWING Solution, sulla piattaforma stessa. Le segnlazioni cartacee vengono conservate da RPCT in un archivio fisico chiuso a chiave. Decorsi i termini di conservazione, le segnalazioni e le eventuali istruttorie sono cancellate (nel caso di segnalazione effettuata tramite l’applicativo WHISTLEBLOWING Solution in modo automatico), irreversibilmente.

## 1.4. Risorse.

### 1.4.1. Quali sono le risorse di supporto ai dati?

Applicativo WHISTLEBLOWING Solution, accessibile da internet

Rete dati interna di AZIENDA SPECIALE RIVIERE DI LIGURIA;

Dispositivi firewall.

### 1.4.2. Persone che possono accedervi.

I dati personali saranno trattati da RPCT e, se del caso, da ODV, specificamente vincolati all’obbligo di riservatezza, con espresso divieto di rivelazione - a persone diverse da quelle specificamente autorizzate - dell’identità del segnalante, in assenza del suo consenso espresso. Previamente individuati e nominati quali “Autorizzati” al trattamento, a tali soggetti sono impartite specifiche istruzioni in ordine a misure e accorgimenti tutti volti alla concreta protezione dei dati personali. La possibilità di accedere ai dati è limitata ai soli soggetti effettivamente legittimati.

Nello specifico:

- RPCT

- ODV

- Responsabile del trattamento ai sensi dell’ art. 28 del Regolamento Europeo n. 679/2016.

Ove, per segnalazioni di particolare complessità il CdA dovesse statuire di costituire il gruppo di lavoro, si prescrive che detto gruppo:

- sia composto da soggetti in possesso di competenze trasversali rispetto ai principali compiti e attività di AZIENDA SPECIALE RIVIERE DI LIGURIA;

- i componenti siano identificati in apposito verbale o atto organizzativo;

- nel codice etico e di comportamento o altro rilevante documento aziendali in vigore in AZIENDA SPECIALE RIVIERE DI LIGURIA siano previste forme di responsabilità specifica in capo ai componenti del gruppo di lavoro (oltre a quella di RPCT e di tutti gli altri soggetti che all’interno di AZIENDA SPECIALE RIVIERE DI LIGURIA possono venire a conoscenza della segnalazione).

Nell’ipotesi in cui RPCT di AZIENDA SPECIALE RIVIERE DI LIGURIA si dovesse trovare in posizione di conflitto di interessi o di impossibilità ad operare il Presidente provvede ad individuare un altro soggetto avente i requisiti di legge e di competenza per procedere alla gestione ed alla analisi della segnalazione

# 2. NECESSITA’ E PROPORZIONALITA’.

## 2.1. Misure previste per garantire il rispetto del GDPR.

Questa valutazione di impatto (DPIA) è effettuata in quanto ha carattere obbligatorio, stante quanto previsto dall’art. 13 comma 6 del D.Lgs 10 marzo 2023, n. 24 “*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*”.

### 2.1.1. Piano di revisione della DPIA.

In generale, si prevede una revisione della presente DPIA nei seguenti casi:

* Violazione dei dati personali
* Modifiche al trattamento, in termini di:
	+ Contesto o finalità del trattamento
	+ Tipologia di dati personali trattati
	+ Destinatari o modalità di raccolta dei dati personali
	+ Combinazioni di dati provenienti da fonti differenti
* Modifica ai rischi con impatto sui diritti degli interessati derivati da:
	+ Presenza di nuove minacce
	+ Modifica ai sistemi informativi a supporto del trattamento
	+ Soppressione di contromisure esistenti
	+ Nuovi scenari di rischio
	+ Nuovi potenziali impatti sulle dimensioni di analisi (Riservatezza, Integrità, Disponibilità)
	+ Attuazioni di nuove misure di sicurezza tecniche, organizzative o procedurali.

### 2.1.2. Applicazione della Privacy by design, principi/strategie.

Il Titolare del trattamento, nell’individuare le misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti in esame, ha definito il proprio modello di gestione delle segnalazioni in conformità ai principi della “protezione dei dati fin dalla progettazione” e della “protezione per impostazione predefinita”.

Quanto sopra risulta anche da:

* informativa/informazioni ex artt. 13 e 14 GDPR;
* misure tecniche adottate.

### 2.1.3. Principi Fondamentali.

Tra i principi fondamentali ex art. 5 del GDPR che il Titolare del trattamento rispetta si annoverano in particolare:

* la trasparenza nei confronti del segnalante e del segnalato (informativa ex artt. 13 e 14 del GDPR);
* la limitazione della conservazione dei dati;
* la limitazione delle finalità;
* la minimizzazione dei dati raccolti.

### 2.1.4. Misure esistenti o pianificate. Politica di tutela della privacy.

AZIENDA SPECIALE RIVIERE DI LIGURIA si è dotata di un Modello Privacy e ha delegato specifici compiti e funzioni connessi al trattamento di dati personali ai referenti delle varie aree aziendali.

Il personale, anche in ragione della sua eseguità, è stato formato con diretto coinvolgimento nella redazione del Modello Privacy e tramite erogazione di modulo formativo.

A titolo esemplificativo e non esaustivo sono state adottate le seguenti procedure aziendali in materia di trattamento dei dati personali:

[-](https://intranet.liguriadigitale.it/components/com_publiccompetitions/includes/download.php?id=41af92b630dcd3e3c67d8c3ba8f1eb191dd66590902c5caaae4776b1ac31e58a34a5aa4391efe99713b44b32c25d56c8f8308aecc2c11a346c16f4ae54b6edba) Gestione delle violazioni di dati personali

- Gestione dei consensi ed informative

[-](https://intranet.liguriadigitale.it/components/com_publiccompetitions/includes/download.php?id=19feebf4f30ceafc88c0e1e79ed6ebf841f8a06a40e26ea83c5073ff9158df22e811be2fc4fbca0d1244fccf4375a483a2c65ea48cced2eb0a88fd13bd0aa9f0) Gestione dell’esercizio dei diritti dell’interessato.

### 2.1.5. Controllo degli accessi fisico e logico.

In primo luogo, nell’ambito della procedura di whistleblowing sono stati previsti presidi organizzativi e/o tecnici che consentano al solo RPCT di associare la segnalazione all’identità del segnalante (pseudonimizzazione).

Premesso che la segnalazione è visibile esclusivamente a RPCT, i singoli canali di segnalazione rispettano i seguenti requisitiil

* la piattaforma WHISTLEBLOWING Solution prevede le seguenti caratteristiche:
* procedure di autenticazione degli utenti
* meccanismo di profilazione degli utenti che consentano solo la visibilità necessaria al ruolo svolto;
* accesso selettivo ai dati delle segnalazioni, con la possibilità per il RPCT di prevedere di assegnare segnalazioni specifiche al singolo soggetto istruttore in funzione di supporto;
* tracciabilità delle operazioni svolte da parte dell’RPCT e dei soggetti istruttori, che non comprende anche le consultazioni che il segnalante effettua sull’evoluzione della propria segnalazione.
* Modalità Orale: in tal caso la segnalazione viene acquisita attraverso un incontro fissato – in locali idonei ad assicurare la riservatezza - ovvero nell’ufficio RPCT;
* Le segnalazioni pervenute sarano protocollate in apposito registro riservato.

Le postazioni di lavoro dalle quali si accede ai sopra citati supporti e gli armadietti ignifughi (chiusi a chiave) in cui viene custodita l’eventuale documentazione cartacea si trovano in locali chiusi e sono gli armadietti sono accessibili al solo RPCT.

## 2.2. Misure che contribuiscono alla proporzionalità e alla necessità. Tracciabilità richieste di accesso.

Il diritto di accesso ai dati personali è esercitabile, così come previsto dall’art. 13 comma 6 del D.Lgs. 24/2023, nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs. 196/2003.

Resta inteso che a norma dell’art. 12 comma 8 del D.Lgs. 24/2023, la segnalazione e l’identità del segnalantesono esclusi dall’accesso ai documenti amministrativi previsto dalla Legge n. 241/1990 e dal D.lgs n. 33/2013.

## 2.3. Finalità determinate, esplicite e legittime.

Laddove vi sia una segnalazione il trattamento delle informazioni e dei dati personali ivi contenuti è obbligatorio.

Il trattamento *de quo* è legittimo, in quanto previsto dalla normativa vigente (in particolare dal D.Lgs. 24/2023). Gli scopi del trattamento sono esplicitati nella documentazione aziendale richiamata e nella presente DPIA al paragrafo “finalità”.

## 2.4. Liceità del trattamento.

Le condizioni di liceità del trattamento effettuato per la succitata finalità sono:

1. obbligo di legge (ex art. 6, par. 1, lett. c), del GDPR), in relazione ai dati comuni;
2. obblighi e diritti del titolare o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale (*ex* art. 9, par. 2, lett. b), del GDPR in relazione ai dati particolari/sensibili;
3. esecuzione di un compito di interesse pubblico contemplato dall’ordinamento (ex art. 10 GDPR e 2-*octies* del Codice Privacy), in relazione ai dati giudiziari.

Peraltro, il trattamento dei dati del dipendente che segnala illeciti, deve essere considerata come una delle “*norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell’ambito dei rapporti di lavoro*” ex art. 88, par. 1, GDPR.

Le basi giuridiche si rinvengono nelle seguenti norme:

- D.Lgs. 24/2023;

- Regolamento Europeo n. 679/2016

- D.Lgs n. 196/2003 come novellato dal D.Lgs n. 101/2018

- D. Lgs. 8 giugno 2001, n. 231

- Legge 30 novembre 2017, n. 179 (integrazione della disciplina dell’obbligo di segreto di ufficio, aziendale, professionale, scientifico ed industriale).

## 2.5. 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 vengono conferiti inizialmente dal segnalante a cui è stato rivolto invito a fornire i soli elementi strettamente necessario e dare seguito alle segnalazioni.

Inoltre il Titolare, fermo che si asterrà dal raccogliere i dati personali manifestamente non utili alla gestione di una specifica segnalazione, provvederà alla loro immediata cancellazione in caso di raccolta accidentale.

Peraltro, i dati raccolti dall’applicativo WHISTLEBLOWING Solution e in modalità orale, sono per loro natura esatti e, se necessario, aggiornati. Il Titolare adotta misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti. Resta inteso che tali diritti sono esercitabili unicamente dal segnalante.

In conclusione, il trattamento risulta conforme al principio di minimizzazione dei dati, atteso che i dati raccolti e conservati risultano essere esclusivamente quelli necessari a conseguire le finalità del trattamento stesso.

Nello svolgimento dell’istruttoria dovrà essere posta particolare cura alla minimizzazione dei dati raccolti da altre fonti anche per non mettere a rischio l’identità del segnalante e del segnalato.

## 2.6. Limitazione della conservazione.

In ossequio al principio di limitazione della conservazione (art. 5, par. 1, lett. e), GDPR), i dati saranno conservati per un periodo non superiore a quello necessario per il perseguimento delle finalità sopra menzionate: vengono conservati per massimo 5 anni decorrenti dalla data della comunicazione dell’esito finale della procedura.

Verrà in ogni caso verificata l’adeguatezza, la pertinenza e l’indispensabilità dei dati rispetto alla segnalazione in corso, da instaurare o cessati, anche con riferimento ai dati che il segnalante fornisce di propria iniziativa. Pertanto, anche a seguito di verifiche, le informazioni e i dati che risultano eccedenti o non pertinenti o non indispensabili non saranno utilizzati, salvo che per l’eventuale conservazione a norma di legge del documento che li contiene.

## 2.7. Misure a tutela dei diritti degli interessati.

### 2.7.1. Come sono informati del trattamento gli interessati?

Gli interessati sono informati tramite apposite informative ex artt. 13 e 14 del GDPR reperibili sul sito internet di AZIENDA SPECIALE RIVIERE DI LIGURIA al link <https://www.asrivlig.it/index.php/altri-contenuti/segnalazione-illeciti-whistleblowing>.

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

In generale, tale trattamento non prevede la raccolta del consenso degli interessati in quanto i dati forniti dal segnalante sono necessari al raggiungimento della finalità per la quale sono forniti.

Nel solo ambito del procedimento disciplinare eventualmente attivato da AZIENDA SPECIALE RIVIERE DI LIGURIA contro il segnalato, l’identità del segnalante non può essere rilevata salvo ricorrano cumulativamente i seguenti fattori

* la contestazione sia fondata, in tutto o in parte, sulla segnalazione;
* la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato;
* il segnalante abbia manifestato il proprio consenso espresso alla rivelazione della sua identità.

In tal caso il consenso viene espresso tramite sottoscrizione del consenso stesso.

### 2.7.2. Come fanno gli interessati a esercitare i loro diritti di cui agli articoli da 15 a 22 GDPR?

In conformità a quanto previsto dall’art. 13 comma 3 del D.Lgs 24/2023, “*i diritti di cui agli articoli da 15 a 22 del GDPR possono essere esercitati nei limiti di quanto previsto dall’articolo 2-undecies lettera f) del D.Lgs. 196/2003*” e, pertanto, non possono essere esercitati 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.

L’art. 2-undecies del D.Lgs. 196/2003 stabilisce al comma 3, in relazione alle specifiche limitazioni ai diritti dell’interessato dallo stesso previste al comma 1 proprio con riferimento all’istituto del whistleblowing, che in tale ipotesi i diritti in questione possono essere esercitati per il tramite del Garante per la protezione dei dati personali con le modalità di cui all’art. 160 del Codice stesso. Sarà il Garante medesimo a effettuare un bilanciamento tra il diritto invocato dal segnalato e la necessità di riservatezza dei dati identificativi del segnalante.

Con speciale riferimento al diritto di accesso ai dati, come già anticipato, la segnalazione è altresì sottratta all’accesso previsto dagli articoli 22 e seguenti della legge 241/1990, nonché dagli artt. 5 e sss del D.Lgs. 33/2013 (art. 12, comma 8 del D.lgs. 24/2023).

Le informazioni relative al trattamento dei dati personali e alla protezione della riservatezza dei segnalanti sono riportate nell’apposita informativa ex art 13 e 14 GDPR. L’apposita istanza ad RPCT è presentata contattando il medesimo secondo le modalità previste dall’informativa.

# 3. RISCHI PER I DIRITTI E LE LIBERTA’ DEGLI INTERESSATI.

## 3.1. Rischi. Individuazione della metrica del rischio.

La metodologia qui utilizzata è quella proposta dall’ENISA, a cui si rimanda.

Il rischio (in seguito R) viene calcolato come segue: **R = f(P,D)** in cui:

* P: corrisponde alla stima della probabilità di accadimento degli eventi che causano la perdita, violazione, diffusione non autorizzata di dati.
* D: indica la stima della gravità dei danni attesi rispetto all’accadimento di un determinato evento.

Le probabilità (P) di avverarsi dell’evento dannoso sono state individuate come segue:

|  |  |  |
| --- | --- | --- |
| **Valore** | **Livello di probabilità** | **Descrizione** |
| **1** | **BASSO** | È improbabile che la minaccia si materializzi |
| **2** | **MEDIO** | C’è una ragionevole possibilità che la minaccia si materializzi |
| **3** | **ALTO** | La minaccia potrebbe materializzarsi |

I livelli di gravità del danno/impatto (D) sono definiti come segue:

|  |  |  |
| --- | --- | --- |
| **Valore** | **Livello di impatto** | **Descrizione** |
| **1** | **BASSO** | Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.).  |
| **2** | **MEDIO** | Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.). |
| **3** | **ALTO** | Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.). |
| **4** | **MOLTO ALTO** | Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.). |

**Competenze dei compilatori.**

L’autore, il valutatore e il validatore della presente DPIA hanno un’adeguata e specifica formazione professionale nell’ambito delle procedure riguardanti la protezione delle persone che segnalano violazioni del diritto dell’Unione (cd. direttiva whistleblowing) e disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

In particolare, gli stessi sono dotati di competenze specialistiche anche in materia di normativa sulla protezione dei dati personali, sicurezza dei dati e delle informazioni, nonché in tema di predisposizione di procedure di gestione.

Inoltre, il Referente Privacy, valutato il contesto del titolare del trattamento, hanno suggerito la metodologia e contribuito alla valutazione della qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché allo sviluppo di conoscenze specifiche.

### 3.1.1. Le fonti di rischio:

La fonte di rischio consiste nella rivelazione da parte del personale autorizzato o nell’accesso accidentale o non autorizzato ai canali e alle segnalazioni stesse.

Le fonti di rischio hanno ad oggetto la vulnerabilità del sistema adottato e, più precisamente, consistono nell’utilizzo di:

* canali di raccolta delle segnalazioni inadeguati;
* comportamenti non consoni degli Autorizzati;
* strumenti di conservazione/archiviazione non sicuri.

Vi è un rischio di perdita di disponibilità dei dati sia per cause accidentali sia per attività malevole anche del segnalato. Il rischio è del tutto marginale con riferimento al canale di segnalazione preferenziale, tramite piattaforma whistleblowing PA.

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

In premessa, per “ritorsione” si intende “*Qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia all’autorità giudiziaria o contabile, o della divulgazione pubblica e che provoca o può provocare, alla persona segnalante o alla persona che ha sporto la denuncia, in via diretta o indiretta, un danno ingiusto, da intendersi come danno ingiustificato.*”

Esempi di comportamenti ritorsivi:

* il licenziamento, la sospensione o misure equivalenti;
* la retrocessione di grado o la mancata promozione;
* il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro;
* la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa;
* le note di merito negative o le referenze negative;
* l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria;
* la coercizione, l'intimidazione, le molestie o l'ostracismo;
* la discriminazione o comunque il trattamento sfavorevole;
* la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione;
* il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine;
* i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche e la perdita di redditi;
* l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l’impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro;
* la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi;
* l'annullamento di una licenza o di un permesso;
* la richiesta di sottoposizione ad accertamenti psichiatrici o medici.

Pertanto, i principali impatti sugli interessati consistono:

1. nella violazione dell’obbligo di riservatezza e del divieto di ritorsioni, da intendersi quale qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione, della denuncia o della divulgazione pubblica della violazione e che può provocare al segnalante un danno ingiusto;
2. nell’impossibilità di dare seguito alla segnalazione;
3. danni fisici, materiali o immateriali;
4. pregiudizio alla reputazione del segnalante/segnalato o altre conseguenze negative ancor prima che venga dimostrata l’estraneità o meno degli stessi ai fatti segnalati. Il rischio non è infatti solo quello di creare un’impressione negativa sugli altri, bensì quello molto più concreto ed afflittivo di perdere affidabilità;
5. nelle ritorsioni contro i volontari e i tirocinanti che potrebbero concretizzarsi, ad esempio, nel non avvalersi più dei loro servizi, nel dare loro referenze di lavoro negative, nel danneggiarne in altro modo la reputazione o le prospettive di carriera.

### 3.1.3. Principali minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati.

La principale minaccia che potrebbe concretizzare il rischio consiste nell’accesso illegittimo ai dati e, eventualmente, nell’utilizzo improprio dei canali di segnalazione.

Il rischio si identifica:

1. nel possibile accesso/modifica/rivelazione dei dati trattati da parte di personale non autorizzato (e, dunque, diverso da RPCT ovvero dall’Autorità Giudiziaria o nell’ambito del procedimento disciplinare nei casi espressamente previsti dalla normativa vigente); con riferimento al canale whistleblowingPA detto rischio è minimizzato tramite la necessità di profilazione utente e autenticazione tramite password;
2. nella possibile perdita dei dati trattati (distruzione accidentale o illegale);
3. in relazione alle fonti di rischio non umane, limitatamente alle segnalazioni in modalità scritta analogica o orale, si osserva che i locali non sono particolarmente soggetti a eventi calamitosi, quali incendio, allagamento, terremoto.

### Stime della probabilità e della gravità.

Alla luce degli impatti potenziali e delle misure pianificate, visto numero di procedimenti, la separazione degli stessi in differenti archivi tra segnalazioni on line o orali e la scelta di un fornitore qualificato ANAC, la conservazione in cloud certificato dei procedimenti, la custodia in armadi ignifughi e chiusi a chiave all’interno di un ufficio riservato, l’utilizzo di sistemi di ctittografia su cartelle protette su server, la gravità del rischio è stimata come "BASSO”;

Riguardo alle minacce, alle fonti di rischio e alle misure pianificate, la probabilità del rischio è stimata come “BASSO”.

La matrice che scaturisce dalla combinazione di probabilità e gravità del danno è rappresentata in figura seguente:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **PROBABILITÀ** | Alta |  |  |  |
| Media |  |  |  |
| Bassa | X(RID) |  |  |
|  | Basso | Medio | Alto/Molto alto |
|  | **IMPATTO** |

Legenda:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | Rischio basso |  | Rischio medio |  | Rischio alto |

**R = RISERVATEZZA I =IDENTITA’ D = DISPONIBILITA’**

## 3.2. Misure previste per gestire i rischi.

Con riferimento alla rivelazione da parte del personale autorizzato, la violazione dell’obbligo di riservatezza è fonte di responsabilità disciplinare, fatta salva ogni ulteriore forma di responsabilità prevista dalla legge. Generalmente, dunque, ancorché l’identità del segnalante non possa essere rivelata senza il suo espresso consenso e la segnalazione sia gestita nella pressoché totalità dei casi sal solo RPCT e da ODV, senza coinvolgimento di ulteriore personale dipendente, tutti coloro che sono coinvolti nella gestione della segnalazione siano tenuti a tutelarne la riservatezza. A tal fine deve essere assicurata:

* Adeguata informativa e formazione del personale eventualmente Autorizzato;
* la minimizzazione dei dati;
* l’utilizzo di sistemi di crittografia;
* il controllo degli accessi fisici e logici;
* l’aggiornamento tecnologico dei canali messi a disposizione per effettuare la segnalazione;
* programmi antivirus e firewall
* effettuazione periodica di test di vulnerabilità

# 4. OPINIONE DELLE PARTI INTERESSATE.

## 4.1. Parere.

L’indice di questo documento e relativi contenuti rispecchiano quanto indicato nell’allegato 2 del WP 248 *(Criteri per una valutazione d’impatto sulla protezione dei dati accettabile)* (cfr. Comitato Europeo per la protezione dei dati, [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 - WP248rev.01](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236)).

Il sottoscritto avv. Gian Luca Ballero Dalla Dea, consultato in qualità di DPO della Società dal Titolare in conformità all’art. 35, par. 2, del GDPR in merito alla Valutazione d’impatto ex artt. 35-36 GDPR (cd. DPIA) sulle attività di trattamento relative alla “*Segnalazione di condotte illecite (whistleblowing)*”, effettuata in data 13/12/2023, nello svolgimento dei compiti attribuitigli da AZIENDA SPECIALE RIVIERE DI LIGURIA fornisce il seguente

**PARERE**

Alla luce di quanto descritto nella presente DPIA e della documentazione sottoposta al DPO, si ritiene che la procedura in questione, laddove effettivamente attuata nei termini indicati, possa essere considerata pienamente rispettosa dei principi di cui all'art. 5 del GDPR. In particolare, le misure di sicurezza applicate, in rapporto alla tipologia di dati trattati, appaiono adeguate a rispettare i dettami dell'art. 32 del GDPR nonché, più in generale, i diritti e le libertà fondamentali degli individui. Il Referente si riserva, comunque, successive valutazioni anche a seguito dei possibili riscontri che potrebbero pervenire dagli interessati. In quest’ottica, qualora la concreta applicazione della Procedura lo richiedesse, dovranno essere implementate eventuali misure correttive che, nel caso, condurranno altresì ad un aggiornamento della presente DPIA.

## 4.2. Conclusioni

La presente valutazione d’impatto sulla protezione dei dati personali (nel proseguo anche “DPIA” – *Data Protection Impact Assessment*) è effettuata in ossequio all’obbligo previsto dall’art. 13, comma 6, del D.lgs. 24/2023 al fine di individuare misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati.

**AZIENDA SPECIALE RIVIERE DI LIGURIA Srl,** Titolare del trattamento, considerati la natura, l’oggetto, il contesto e le finalità del trattamento relativo alle procedure del whistleblowing, ritiene che siano state messe in atto garanzie e misure tecnico-organizzative adeguate che presentano **un rischio basso per i diritti e le libertà degli interessati**