COMUNE DI ALBISSOLAMARINA

WHISTLEBLOWING

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

(art. 35 Regolamento UE 2016/679
art. 13 D.Lgs. 10.03.2023, n. 24)

TITOLARE DEL TRATTAMENTO: **COMUNE DI ALBISSOLA MARINA**

AREA/SETTORE/SERVIZIO: **SEGRETERIA GENERALE**

DIRIGENTE/RESPONSABILE: **SEGRETARIO GENERALE**

DATA DEL DOCUMENTO: 25.11.2024

APPROVATO CON DELIBERA DI GIUNTA N. 125 DEL 28/11/2024

RESPONSABILE PROTEZIONE DATI (RPD): Avv. Massimo Ramello

Sommario

A. IN GENERALE

La Valutazione d'impatto sulla protezione dei dati rappresenta una delle principali novità introdotte dalla recente normativa in materia di protezione dei dati personali, in quanto correlata al principio generale di responsabilizzazione del Titolare del trattamento (accountability).

La Valutazione di impatto sulla protezione dei dati personali (nel seguito DPIA) è un processo che permette di valutare il livello di esposizione al rischio associato al trattamento dei dati personali e la necessità e proporzionalità del trattamento medesimo al fine di garantire e dimostrare la conformità dell'attività di trattamento con le prescrizioni normative.

A.1. Il Decreto

Il Decreto Legislativo 10 marzo 2023, n. 24 (di seguito, per brevità, "Decreto") recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione.

La nuova disciplina è orientata, da un lato, a garantire la manifestazione della libertà di espressione e di informazione, che comprende il diritto di ricevere e di comunicare informazioni, nonché la libertà e il pluralismo dei media. Dall'altro, è strumento per contrastare (e prevenire) la corruzione e la cattiva amministrazione nel settore pubblico e privato.

Chi segnala fornisce informazioni che possono portare all'indagine, all'accertamento e al perseguimento dei casi di violazione delle norme, rafforzando in tal modo i principi di trasparenza e responsabilità delle istituzioni democratiche.

Pertanto, garantire la protezione – sia in termini di tutela della riservatezza che di tutela da ritorsioni - dei soggetti che si espongono con segnalazioni, denunce o, come si vedrà, con il nuovo istituto della divulgazione pubblica, contribuisce all'emersione e alla prevenzione di rischi e situazioni pregiudizievoli per la stessa amministrazione o ente di appartenenza e, di riflesso, per l'interesse pubblico collettivo.

Tale protezione viene, ora, ulteriormente rafforzata ed estesa a soggetti diversi da chi segnala, come il facilitatore o le persone menzionate nella segnalazione, a conferma dell'intenzione, del legislatore europeo e italiano, di creare condizioni per rendere l'istituto in questione un importante presidio per la legalità e il buon andamento delle amministrazioni/enti.

A.2. Il RGPD

Il trattamento dei dati personali raccolti attraverso i canali di segnalazione interni di cui all'art. 4 del Decreto, comporta l'applicabilità della normativa di protezione contenuta nel **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 o RGPD).

L'**articolo 13, comma 1 del Decreto** stabilisce che "*Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51*".

L'**articolo 13, comma 6, del Decreto** prevede che "*I soggetti di cui all'articolo 4 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, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*".

L'**articolo 35 del RGPD** impone al Titolare di effettuare la DPIA prima di iniziare una data attività di trattamento che possa comportare "*un rischio elevato per i diritti e le libertà delle persone*", in particolare

quando prevede di avviare un trattamento mediante "*utilizzo di nuove tecnologie, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità del trattamento*".

L'**articolo 35 del RGPD** fa riferimento al possibile rischio elevato "*per i diritti e le libertà delle persone fisiche*". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "*diritti e libertà*" degli interessati riguarda principalmente i diritti alla protezione dei dati ed alla vita privata, ma include anche altri diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.

In linea generale il RGPD aiuta a comprendere come le casistiche di rischio possano avere probabilità e gravità diverse e derivare da attività di trattamento suscettibili di arrecare pregiudizi fisici, materiali o immateriali, in particolare se il trattamento possa comportare "*discriminazioni, furto o usurpazione d'identità, perdite finanziarie, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale, decifratura non autorizzata della pseudonimizzazione, o qualsiasi altro danno economico o sociale significativo*", la perdita di controllo da parte dell'interessato sui dati personali che li riguardano o privazioni o limitazioni nell'esercizio dei propri diritti fondamentali e libertà (v. **Considerando 75 del RGPD**).

La probabilità e la gravità del rischio per i diritti e le libertà dell'interessato dovrebbero essere determinate avendo riguardo "*alla natura, all'ambito di applicazione, al contesto e alle finalità del trattamento*" (v. **Considerando 76 del RGPD**).

Dunque, occorrerà valutare se il trattamento riguardi "*dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza*" o sia finalizzato a valutare aspetti personali "*in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali*" o se si riferisca a "*dati personali di persone fisiche vulnerabili, in particolare minori*" o se riguardi "*una notevole quantità di dati personali e un vasto numero di interessati*" (v. **Considerando 75 del RGPD**).

Con riferimento ai trattamenti "*su larga scala*", ossia relativi ad una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potenzialmente presentano un rischio elevato, il RGPD incentra l'attenzione sulle categorie di dati particolari o sulle finalità delle attività di trattamento "*per adottare decisioni riguardanti determinate persone fisiche in seguito a una valutazione sistematica e globale di aspetti personali relativi alle persone fisiche, basata sulla profilazione di tali dati, o in seguito al trattamento di categorie particolari di dati personali, dati biometrici o dati relativi a condanne penali e reati o a connesse misure di sicurezza*" (v. **Considerando 91 del RGPD**).

Infine, particolare attenzione deve essere posta su quei trattamenti che "*comportano l'utilizzo di nuove tecnologie o quelli che sono di nuovo tipo e in relazione ai quali il titolare del trattamento non ha ancora effettuato una valutazione d'impatto sulla protezione dei dati, o la valutazione d'impatto sulla protezione dei dati si riveli necessaria alla luce del tempo trascorso dal trattamento iniziale*" (v. **Considerando 89 del RGPD**).

Il valore ed il ruolo della DPIA sono altresì chiariti nel **RGPD** all'interno del **Considerando n. 84** nei termini seguenti: "*Per potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio*".

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

Più nello specifico il documento illustra le considerazioni logiche che hanno accompagnato le fasi di identificazione, valutazione e risposta a tutti i rischi rilevati all'interno del trattamento oggetto di analisi.

Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.

Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'**articolo 36 del RGPD**, dando luogo alla c.d. consultazione preventiva.

Il mancato svolgimento della DPIA quando il trattamento è soggetto a tale valutazione (**articolo 35, paragrafi 1, 3 e 4 del RGPD**), lo svolgimento non corretto di una DPIA (**articolo 35, paragrafi 2, 7 e 9 del RGPD**) o la mancata consultazione dell'autorità di controllo competente ove ciò sia necessario (**articolo 36, paragrafo 3, lettera e) del RGPD** possono comportare l'irrogazione di una sanzione amministrativa pecuniaria fino a un massimo di 10 milioni di Euro, ovvero – se si tratta di un'impresa – fino al 2% del fatturato mondiale totale annuo dell'esercizio finanziario precedente, se superiore alla citata soglia del 10 milioni di Euro.

A.3. Altre fonti normative

Disposizioni rilevanti in materia sono altresì contenute nei seguenti provvedimenti:

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 (di seguito: **Linee guida WP248**), adottate il 4 aprile 2017 e come modificate e adottate da ultimo il 4 ottobre 2017;

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI - Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679 (di seguito: **Linee guida WP250**), adottate il 3 ottobre 2017 ed emendate e adottate da ultimo in data 6 febbraio 2018;

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - parere favorevole sullo "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" predisposto da ANAC. Adottato il 6 luglio 2023;

AUTORITA' NAZIONALE ANTICORRUZIONE (ANAC) - 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 - Approvate con Delibera n°311 del 12 luglio 2023

A.4. Metodologia

I contenuti minimi della DPIA sono specificati come segue all'**articolo 35, paragrafo 7 del RGPD**:
a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

La metodologia qui adottata per la valutazione di impatto sulla protezione dei dati personali (DPIA), ai sensi dell'art. 35 RGPD, è sviluppata sulla base di quella definita da:
- **Commission nationale de l'informatique et des libertés o CNIL**, l'Autorità francese per la protezione dei dati, in conformità alle Linee guida WP248 e inclusa tra le metodologie raccomandate nell'allegato 1 delle Linee guida stesse;
- **Information Commissioner's Office o ICO**, l'Autorità inglese per la protezione dei datipersonali;

Al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti 'interessati', si è proceduto alla valutazione dell'effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di iniziative finalizzate all'adempimento degli obblighi dettati dal citato regolamento per la protezione dei dati, altresì noto come GDPR. Lo schema adottato è il seguente:
· la descrizione sistematica del trattamento e delle finalità;
· la descrizione della natura, dell'ambito, del contesto e degli scopi del trattamento;
· i dati personali trattati, i destinatari e il periodo per il quale sono conservati;
· una descrizione funzionale dell'operazione di trattamento;
· la descrizione dell'asset model su cui si basano i dati personali (es. Siti, hardware, software, reti, organizzazione, ecc.);
· la valutazione della necessità e la proporzionalità del trattamento;
· la descrizione delle misure previste per conformarsi al regolamento;
· la descrizione del modo in cui sono gestiti i rischi per i diritti e le libertà degliinteressati;
· la descrizione dell'origine, della natura, della particolarità e della gravità dei rischi;
· la determinazione delle misure previste per il trattamento di tali rischi;
· la descrizione del modo in cui sono coinvolte le parti interessate;
· il parere del Responsabile della Protezione dei Dati Personali (RPD);
· le opinioni eventualmente raccolte dagli interessati o dei loro rappresentanti

B. ANALISI PRELIMINARE DEL TRATTAMENTO OGGETTO DI VALUTAZIONE

L'analisi preliminare del trattamento è la prima fase del processo di valutazione del rischio ed è finalizzata a discriminare i trattamenti di dati personali che evidenziano un rischio elevato da quelli caratterizzati un rischio minore (di livello basso o medio). Essa serve quindi a **raccogliere le principali informazioni relative a uno specifico trattamento di dati personali** ed a decidere se esso debba essere sottoposto alla (sola) valutazione del rischio (in caso di rischio basso o medio per i diritti e le libertà delle persone fisiche) o alla DPIA (in caso di rischio elevato per i diritti e le libertà delle persone fisiche).

B.1. DESCRIZIONE SISTEMATICA DEL TRATTAMENTO (art. 35, paragrafo 7, lettera a) del RGPD)

Indicazioni di **metodo**:
1. si tiene conto della natura, dell'ambito, del contesto e delle finalità del trattamento (**considerando 90 del RGPD**);
2. si dà una descrizione funzionale del trattamento;
3. sono indicati i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi;
4. si specificano gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);
5. si tiene conto dell'osservanza di codici di condotta approvati (**art. 35, paragrafo 8, del RGPD**);

B.1.1 Il trattamento oggetto di analisi e valutazione è rappresentato da:

Canali di segnalazione interni, istituiti in conformità a quanto previsto dall'articolo 4 del Decreto, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

In particolare, i canali adottati dal Titolare sono:

X	Piattaforma informatica
	Posta elettronica
	Posta elettronica certificata (PEC)
	Linea telefonica dedicata, con registrazione
	Sistema di messaggistica vocale
	Incontro diretto, fissato entro un termine ragionevole
X	Consegna diretta al protocollo
X	Spedizione a mezzo posta (o corriere)

La descrizione delle caratteristiche tecniche della piattaforma informatica è contenuta nella documentazione progettuale ed esecutiva allegata alla presente DPIA.

Di seguito sono evidenziate le **caratteristiche di maggior rilevanza sotto il profilo della protezione dei dati personali**.

B.1.2. Rilevanza “quantitativa” in termini di interessati

Il perimetro di applicazione soggettivo della normativa di protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato è stabilito dall’articolo 3 del Decreto.

Il Decreto amplia notevolmente, rispetto alla precedente normativa, i soggetti cui, all’interno del settore pubblico, è riconosciuta protezione, anche da ritorsioni, in caso di segnalazione, interna o esterna, divulgazione pubblica e denuncia all’Autorità giudiziaria. Vi sono ricompresi, tra l’altro, tutti i soggetti che si trovino anche solo temporaneamente in rapporti lavorativi con una amministrazione o con un ente privato, pur non avendo la qualifica di dipendenti (come i volontari, i tirocinanti, retribuiti o meno), gli assunti in periodo di prova, nonché coloro che ancora non hanno un rapporto giuridico con gli enti citati o il cui rapporto è cessato se, rispettivamente, le informazioni sulle violazioni sono state acquisite durante il processo di selezione o in altre fasi precontrattuali ovvero nel corso del rapporto di lavoro.

B.1.3. Dati personali

La gestione dei canali di segnalazione interni implica il trattamento di dati personali, nell’accezione contenuta all’**articolo 4 del GDPR paragrafo 1, n. 1 del RGPD**.

In particolare, il trattamento riguarda i dati personali raccolti in conseguenza delle segnalazioni pervenute al Titolare, nonché quelli riguardanti il personale che, attraverso l’utilizzo di detti canali, provveda alla gestione delle segnalazioni medesime.

Di seguito sono elencate le categorie di dati personali oggetto di trattamento, distinte in ragione di quanto previsto dagli **articoli 6, 9 e 10 del RGPD** (al fine della verifica delle condizioni di liceità del trattamento).

CATEGORIE DI DATI PERSONALI TRATTATE

X	Dati identificativi (cognome, nome, data di nascita, ecc.)
X	Dati di contatto (numeri telefonici, recapiti elettronici, ecc.)
X	Dati relativi al rapporto di lavoro, di servizio o libero professionale
X	Modalità di svolgimento di fatti costituenti illecito

Categorie particolari di dati personali

In talune circostanze può verificarsi che la gestione delle segnalazioni pervenute al Titolare determini il trattamento di dati c.d. "sensibili", nell'accezione di cui all'**articolo 9 del RGPD**. In particolare:

X	Dati personali che rivelino l'origine razziale o etnica
X	Dati personali che rivelino le opinioni politiche, le convinzioni religiose o filosofiche
X	Dati personali che rivelino l'appartenenza sindacale
N.A.	Dati genetici
N.A.	Dati biometrici intesi a identificare in modo univoco una persona fisica
X	Dati relativi alla salute
X	Dati relativi alla vita sessuale
X	Dati relativi all'orientamento sessuale della persona

Dati giudiziari

Le particolari finalità che impongono l'istituzione e legittimano l'utilizzo dei canali di segnalazione interni rendono altamente probabile il trattamento di dati personali relativi alla commissione di reati, nell'accezione di cui all'**articolo 10 del RGPD**.

B.1.4. Operazioni (modalità) del trattamento

A norma dell'**articolo 4, paragrafo 1, n. 2 del RGPD**:
per "*trattamento*" s'intende "*qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione*".

Di seguito sono elencate le operazioni di trattamento, comunemente, attuate dal Titolare:

X	Raccolta
X	Registrazione
X	Organizzazione
X	Strutturazione
X	Conservazione
X	Adattamento o modifica
X	Estrazione
X	Consultazione
X	Uso
X	Comunicazione mediante trasmissione
N.A.	Diffusione o qualsiasi altra forma di messa a disposizione
X	Raffronto
N.A.	Interconnessione
N.A.	Limitazione
X	Cancellazione
X	Distruzione
N.A.	Profilazione o scoring (Il riferimento è a meccanismi di profilazione o algoritmi predittivi che possano ad esempio impattare sulla situazione economica, sulla salute, sugli interessi personali,

	sul comportamento, sull'ubicazione, sugli spostamenti, sulle abitudini di consumo, sul rendimento professionale, ecc.)
N.A.	Adozione di decisioni automatizzate che possano produrre effetti giuridici per i destinatari, senza l'intervento di decisione umana

Particolare attenzione va posta in relazione a specifiche operazioni di trattamento, di seguito individuate:

I dati personali sono **raccolti**:

X	Presso l'interessato
X	Presso soggetti diversi dall'interessato

Criteri di **conservazione** dei dati personali

X	Per le segnalazioni su piattaforma informatica, 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del RPCT, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte
X	Per tutte le segnalazioni, il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione

La **cancellazione** dei dati personali al termine del periodo di conservazione avviene

X	Con procedure automatizzate, limitatamente ai dati trattati mediante piattaforma informatica
X	Con procedure manuali
N.A.	Con procedure in parte automatizzate ed in parte manuali

I dati raccolti attraverso i canali di segnalazione interni possono essere **comunicati**, nel rispetto delle norme di legge e regolamentari, a:

		Note
Autorità giudiziaria	**X**	
Corte dei Conti	**X**	
ANAC	**X**	
Segnalato	**X**	articolo 12, comma 5, del Decreto
Interessato	**X**	articolo 2-undecies del D.Lgs. 30 giugno 2003, n. 196

Diffusione dei dati personali:

X	Non è prevista alcuna forma di diffusione delle informazioni raccolte attraverso i canali di segnalazione interni

L'utilizzo dei canali di segnalazione interni comporta il **trasferimento di dati all'estero**:

X	NO
N.A.	SI, in ragione dell'utilizzo di servizi "Cloud", i dati sono trasferiti verso un paese europeo
N.A.	SI, in ragione dell'utilizzo di servizi "Cloud", i dati sono trasferiti verso un paese terzo od un'organizzazione internazionale

B.1.5. Liceità del trattamento

Al fine di valutare la liceità del trattamento, occorre individuare dettagliatamente le finalità del trattamento (**articolo 5, paragrafo 1, lettera b) del RGPD**).

Le finalità del trattamento sono esplicite, specifiche e legittime. In particolare,
- sono **esplicite**: in quanto sono individuate all'interno del Decreto e sono indicate con chiarezza nelle informazioni rese all'interessato ai sensi degli **articoli 13 e 14 del RGPD**;
- sono **specifiche**: in quanto si riferiscono a tutti i canali di segnalazione interni istituiti dal Titolare;
- sono **legittime**: in quanto trovano adeguato fondamento nelle disposizioni contenute negli **articoli 6, 9 e 10 del RGPD**.

Il Titolare ha adottato un proprio documento organizzativo, con Delibera di Giunta n. 215 in data 20.12.2023.

Finalità del trattamento:

X	Acquisizione delle segnalazioni pervenute attraverso i canali di segnalazione interni
X	Documentazione delle segnalazioni orali
X	Gestione delle comunicazioni con gli interessati
X	Gestione delle comunicazioni con le Autorità competenti in materia
X	Non sono previste operazioni di trattamento successive alla raccolta, incompatibili con lo scopo iniziale

Il trattamento dei dati personali conseguente all'attivazione dei canali di segnalazione interni trova un adeguato fondamento nelle **basi giuridiche** di seguito elencate.

Il trattamento dei dati personali (**comuni**) avviene in quanto:

X	l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità (articolo 6, par. 1, lett. a) del RGPD)
N.A.	il trattamento è necessario all'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso (articolo 6, par. 1, lett. b) del RGPD)
X	il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento (articolo 6, par. 1, lett. c) del RGPD)
N.A.	il trattamento è necessario per la salvaguardia degli interessi vitali dell'interessato o di un'altra persona fisica (articolo 6, par. 1, lett. d) del RGPD)
X	il trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento (articolo 6, par. 1, lett. e) del RGPD)
N.A.	il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato che richiedono la protezione dei dati personali, in particolare se l'interessato è un minore (articolo 6, par. 1, lett. f) del RGPD)

Il trattamento dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona (**sensibili**) avviene in quanto:

N.A.	Non è previsto il trattamento di categorie particolari di dati personali

X	l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche (articolo 9, par. 2, lett. a) del RGPD)
N.A.	il trattamento è necessario per 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 (articolo 9, par. 2, lett. b) del RGPD)
N.A.	il trattamento è necessario per tutelare un interesse vitale dell'interessato o di un'altra persona fisica qualora l'interessato si trovi nell'incapacità fisica o giuridica di prestare il proprio consenso (articolo 9, par. 2, lett. c) del RGPD)
N.A.	il trattamento è effettuato, nell'ambito delle sue legittime attività e con adeguate garanzie, da una fondazione, associazione o altro organismo senza scopo di lucro che persegua finalità politiche, filosofiche, religiose o sindacali, a condizione che il trattamento riguardi unicamente i membri, gli ex membri o le persone che hanno regolari contatti con la fondazione, l'associazione o l'organismo a motivo delle sue finalità e che i dati personali non siano comunicati all'esterno senza il consenso dell'interessato (articolo 9, par. 2, lett. d) del RGPD)
N.A.	il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato (articolo 9, par. 2, lett. e) del RGPD)
N.A.	il trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria o ogniqualvolta le autorità giurisdizionali esercitino le loro funzioni giurisdizionali (articolo 9, par. 2, lett. f) del RGPD)
X	il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, par. 2, lett. g) del RGPD)
N.A.	il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro, valutazione della capacità lavorativa del dipendente, diagnosi, assistenza o terapia sanitaria o sociale ovvero gestione dei sistemi e servizi sanitari o sociali sulla base del diritto dell'Unione o degli Stati membri o conformemente al contratto con un professionista della sanità (articolo 9, par. 2, lett. h) del RGPD)
N.A.	il trattamento è necessario per motivi di interesse pubblico nel settore della sanità pubblica, quali la protezione da gravi minacce per la salute a carattere transfrontaliero o la garanzia di parametri elevati di qualità e sicurezza dell'assistenza sanitaria e dei medicinali e dei dispositivi medici, sulla base del diritto dell'Unione o degli Stati membri che prevede misure appropriate e specifiche per tutelare i diritti e le libertà dell'interessato, in particolare il segreto professionale (articolo 9, par. 2, lett. i) del RGPD)
X	il trattamento è necessario a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici in conformità dell'articolo 89, paragrafo 1, sulla base del diritto dell'Unione o nazionale, che è proporzionato alla finalità perseguita, rispetta l'essenza del diritto alla protezione dei dati e prevede misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato (articolo 9, par. 2, lett. j) del RGPD)

Il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza (**giudiziari**) avviene in quanto:

N.A.	Non è previsto il trattamento di dati a carattere giudiziario
X	Sotto il controllo dell'autorità pubblica
X	E' autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati

B.1.6. Necessità del trattamento

Il Titolare del trattamento ha valutato se questa **misura** fosse, in primo luogo, **idonea** al perseguimento delle finalità indicate e, in secondo luogo, se la misura fosse **adeguata** e **necessaria** per i propri scopi.

L'istituzione di canali interni per la raccolta e la gestione di segnalazioni è prevista dal Decreto Legislativo 10 marzo 2023, n. 24.

B.1.7. Soggetti del trattamento

B.1.7.1. Categorie di interessati

Il trattamento riguarda le seguenti categorie:

X	Persone fisiche segnalanti
X	Persone indicate come possibili responsabili delle condotte illecite
X	Persone fisiche a vario titolo coinvolte nelle vicende segnalate
X	Persone fisiche autorizzate alla gestione dei canali di segnalazione interni
N.A.	Persone fisiche autorizzate ad operare sui sistemi informatici interessati (Amministratori di sistema interni alla struttura organizzativa del Titolare)

B.1.7.2. Titolare del trattamento

Titolare del trattamento è: Avv. Gianluca Nasuti, Sindaco del Comune di Albissola Marina;

Il Titolare è soggetto con sede nell'Unione Europea; non necessita, pertanto, la nomina di un Rappresentante. In ottemperanza all'obbligo contenuto nell'articolo 37 del RGPD, il Titolare ha proceduto all'individuazione del **Responsabile della Protezione dei Dati Personali (RPD)**, alla comunicazione dei relativi dati di contatto al Garante per la protezione dei dati personali ed alla loro pubblicazione sul proprio sito web istituzionale

- l'identificazione di soggetti autorizzati al trattamento con assegnazione di specifiche istruzioni, ai sensi dell'**articolo 29 del RGPD**;
- attribuzione ad uno o più soggetti determinati di specifici compiti e funzioni connessi al trattamento di dati personali, ai sensi dell'**articolo 2-quaterdecies del Codice privacy**.

Con riferimento al **personale** operante sotto la propria autorità, il Titolare ha previsto:
Soggetti che operano sotto l'autorità del Titolare del trattamento:

X	Il Responsabile della Prevenzione della Corruzione e della Trasparenza

Autorizzati al trattamento

N.A.	Sindaco o suo delegato
N.A.	Personale appartenente al corpo di Polizia Locale
N.A.	Personale appartenente al servizio Tecnico
N.A.	Personale appartenente al servizio Sociale
N.A.	Personale appartenente al servizio Personale

Amministratore di sistema

N.A.	Il Titolare non ha designato un amministratore di sistema
N.A.	Il Titolare ha designato un amministratore di sistema all'interno della propria struttura organizzativa
X	Il Titolare ha designato un amministratore di sistema all'interno della struttura organizzativa del Responsabile del trattamento (e sub-responsabili)
N.A.	L'amministratore di sistema è designato in relazione all'intero sistema informatico del Titolare

B.1.7.3. Contitolare del trattamento

L'**articolo 26 del RGPD** dispone che:
"*1. **Allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono contitolari del trattamento**. Essi determinano in modo trasparente, mediante un **accordo interno**, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal presente regolamento, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli articoli 13 e 14, a meno che e nella misura in cui le rispettive responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. Tale accordo può designare un punto di contatto per gli interessati.*

2. L'accordo di cui al paragrafo 1 riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.
3. Indipendentemente dalle disposizioni dell'accordo di cui al paragrafo 1, l'interessato può esercitare i propri diritti ai sensi del presente regolamento nei confronti di e contro ciascun titolare del trattamento".

L'**articolo 4, comma 4, del Decreto** stabilisce che "*I comuni diversi dai capoluoghi di provincia possono condividere il canale di segnalazione interna e la relativa gestione. I soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a "duecentoquarantanove", possono condividere il canale di segnalazione interna e la relativa gestione*".
L'**articolo 13, comma 5, del Decreto** prevede che "*I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018*".

Nella gestione dei canali di segnalazione interni:

X	Non è previsto alcun rapporto di contitolarità
N.A.	E' in fase di valutazione la necessità od opportunità di un trattamento congiunto ad altri
N.A.	E' previsto un rapporto di contitolarità

B.1.7.4. Responsabile del trattamento

L'**articolo 28 del RGPD** dispone che:
"*1. **Qualora un trattamento debba essere effettuato per conto del titolare del trattamento**, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino 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.*
(...)
*3. **I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

Nell'istituzione dei canali di segnalazione interni:

N.A.	Non si fa ricorso ad alcun soggetto esterno che tratti dati personali per conto del Titolare
N.A.	Il trattamento dei dati per conto del Titolare è affidato ad un soggetto pubblico
X	Il trattamento dei dati per conto del Titolare è affidato ad un soggetto privato nel contesto di un servizio di assistenza e/o manutenzione
X	Il trattamento dei dati per conto del Titolare avviene in conseguenza dell'utilizzo di un servizio "Cloud"

Estremi identificativi del/i Responsabile/i e descrizione del trattamento:

WHISTLEBLOWING SOLUTIONS I.S. S.R.L., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961

B.1.7.5. Altro Responsabile del trattamento

L'**articolo 28 del RGPD** dispone che:
"*2. **Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta**, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche.*
(…)
*4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, **su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico** a norma del diritto dell'Unione o degli Stati membri, **gli stessi obblighi in materia di protezione dei dati** contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile*".

Nell'istituzione dei canali di segnalazione interni:

N.A.	Non è previsto il ricorso ad altri responsabili (sub-responsabili)
N.A.	Non è consentito il ricorso ad altri responsabili (sub-responsabili)
N.A.	E' consentito il ricorso ad altri responsabili (sub-responsabili), previa autorizzazione generale
X	In relazione all'utilizzo della piattaforma informatica, è consentito il ricorso ad altri responsabili (sub-responsabili), previa autorizzazione specifica
X	In relazione all'utilizzo della piattaforma informatica, in caso di sostituzione degli altri responsabili (sub-responsabili), è prevista l'informativa al Titolare
X	Il Responsabile ha sottoscritto un accordo sul trattamento dei dati personali con gli altri responsabili (sub-responsabili) autorizzati

Estremi identificativi degli altri responsabile e descrizione del trattamento:

TRANSPARENCY INTERNATIONAL ITALIA, con sede in P.le Carlo Maciachini 11 - 20159 Milano (CF: 97186250151), come partner di progetto con funzione di supporto agli utenti ed Amministratore di Sistema (https://www.transparency.it/chi-siamo)
SEEWEB SRL, con sede in Milano, Via Caldera 21 (CF/PIVA: 02043220603) come fornitore di infrastruttura con funzioni di archiviazione Hosting Cloud IASS e Backup (https://www.seeweb.it/azienda/chi-siamo)

B.2. VALUTAZIONE DELLA CONFORMITA' DEL TRATTAMENTO

Raccolte tutte le informazioni utili a identificare e censire il trattamento, si rende necessaria l'**analisi della necessità e della proporzionalità** del trattamento rispetto alle finalità.

B.2.1. verifica circa il rispetto del GDPR

Sono sottoposti a verifica i seguenti aspetti:

B.2.1.1. il trattamento rispetta i princìpi applicabili al trattamento dei dati personali (CAPO II del GDPR)

In relazione alle **FINALITÀ** del trattamento:

X	Le finalità sono chiaramente previste nel Decreto e nell'atto organizzativo del Titolare
X	Le finalità sono chiaramente indicate nell'informativa
X	Le finalità sono specificamente individuate in relazione a tutti i canali di segnalazione
X	Il perseguimento delle finalità è conforme alla normativa di riferimento per il Titolare
X	I dati personali sono raccolti per le sole finalità indicate nell'informativa fornita all'Interessato del trattamento
X	Il trattamento risulta proporzionato e non eccedente rispetto le relative finalità. Infatti, lo stesso non concerne alcuna finalità ulteriore rispetto quelle esplicitate nell'informativa resa all'Interessato ai sensi dell'articolo 13 del RGPD

Le **BASI GIURIDICHE** del trattamento sono individuate e descritte.
I trattamenti di dati personali posti in essere dal Titolare, nell'ambito della gestione dei canali di segnalazione interni, sono necessari per dare attuazione agli **obblighi di legge** ed ai **compiti d'interesse pubblico** previsti dalla disciplina di settore, la cui osservanza è condizione di liceità del trattamento (artt. 6, par. 1, lett. c) ed e) e parr. 2 e 3, 9, par. 2, lett. b) e g), 10 e 88 del RGPD, nonché 2-ter e 2-sexies del Codice).
In talune circostanze, di seguito riassunte, è prevista l'acquisizione del **consenso** dell'Interessato.
L'identità della persona segnalante e qualsiasi altra informazione da cui può evincersi, direttamente o indirettamente, tale identità non possono essere rivelate, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati (articolo 12, comma 2, del Decreto).
Nell'ambito del procedimento disciplinare, qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità (articolo 12, comma 5, del Decreto).
Se per la segnalazione si utilizza una linea telefonica registrata o un altro sistema di messaggistica vocale registrato, la segnalazione, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante trascrizione integrale (articolo 14, comma 2, del Decreto).
Quando, su richiesta della persona segnalante, la segnalazione è effettuata oralmente nel corso di un incontro con il personale addetto, essa, previo consenso della persona segnalante, è documentata a cura del personale addetto mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale (articolo 14, comma 4, del Decreto).

CICLO DI VITA DEL TRATTAMENTO DEI DATI (descrizione funzionale)
Secondo quanto previsto dal documento organizzativo adottato dal Titolare, la gestione dei canali di segnalazione interna è affidata, in ossequio alla previsione contenuta nel comma 5 dell'art. 4 del Decreto, al Responsabile Prevenzione Corruzione e Trasparenza (RPCT), il quale può avvalersi di personale

espressamente autorizzato a ricevere o a dare seguito alle segnalazioni, ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196. Tale autorizzazione terrà conto del principio del privilegio minimo (PoLP), mutuato dall'ambiente della sicurezza delle informazioni, secondo il quale, ad un utente, vengono concessi i livelli – o permessi – minimi di accesso dei quali ha bisogno per svolgere le proprie mansioni.

Il Titolare intende favorire il ricorso all'istituto del whistleblowing, assicurando molteplicità di canali disponibili e adeguate procedure gestionali quali:

a) una piattaforma informatica;
b) segnalazioni a mezzo posta o consegna diretta;
c) appuntamento con il RPCT

In relazione alla **QUALITÀ** dei dati personali trattati

X	I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati
X	La piattaforma informatica è configurata in modo da limitare il numero di informazioni la cui raccolta è necessaria per completare la procedura
X	La piattaforma informatica è configurata in modalità "Custode dell'identità" con limitazione dell'accesso ai dati identificativi del segnalante

ADEGUATEZZA, PERTINENZA E LIMITAZIONE dei dati trattati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati):

X	La piattaforma informatica consente al segnalante la scelta se procedere alla segnalazione in forma anonima o nominativa
X	La piattaforma informatica integra la tecnologia "TOR"
X	La piattaforma informatica è configurata in modo da non consentire il tracciamento degli utenti che vi accedano dall'interno della rete aziendale
X	La piattaforma informatica è configurata per non registrare gli indirizzi IP di navigazione e User agent
X	La piattaforma informatica non lascia tracce nella cache del browser
X	La piattaforma informatica è configurata per consentire l'accesso del segnalante alle proprie segnalazioni, senza necessità di effettuare un'autenticazione (mediante inserimento del solo Codice Univoco)
X	In caso di consegna della segnalazione con modalità analogiche (consegna diretta o a mezzo posta) sono impartite istruzioni al segnalante al fine di limitare l'accesso alla propria identità da parte del ricevente
X	In caso di consegna della segnalazione con modalità analogiche (consegna diretta o a mezzo posta) è prevista una protocollazione riservata
X	I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente

ESATTEZZA ED AGGIORNAMENTO dei dati trattati:

X	La piattaforma informatica è configurata per consentire l'accesso del segnalante alle proprie segnalazioni (mediante inserimento del solo Codice Univoco)
X	Il contenuto delle segnalazioni effettuate in modalità analogiche è verificabile ed aggiornabile dal segnalante mediante richiesta al Titolare

L'**ACCESSO ALLE INFORMAZIONI PERSONALI**, da parte del personale del Titolare, è effettuato:

X	d'ufficio, al ricevimento di una segnalazione
X	d'ufficio, al ricevimento di integrazioni documentali ed informative da parte del segnalante
X	su richiesta di incontro da parte del segnalante
X	d'ufficio con cadenza periodica

In relazione alla **CONSERVAZIONE** dei dati personali trattati

X	il periodo di conservazione è limitato/idoneo ai fini per cui è stato effettuato il trattamento
X	I dati contenuti nelle segnalazioni effettuate mediante piattaforma informatica e quelli identificativi del segnalante (ove presenti) sono conservati all'interno della stessa
X	I dati di accesso alla piattaforma (e relative operazioni) sono conservati all'interno della stessa in una sezione accessibile ai soli Amministratori di sistema
X	I dati contenuti nelle segnalazioni effettuate mediante modalità analogiche e quelli identificativi del segnalante (ove presenti) sono conservati in archivi dedicati, protetti da serratura, ad accesso riservato al RPCT e soggetti da questo eventualmente delegati

Con particolare riferimento alle **FIGURE SOGGETTIVE** coinvolte:

X	Sono stati individuate, autorizzate ed istruite le risorse umane deputate al trattamento mediante piattaforma informatica (RPCT, soggetti dal medesimo delegati ed amministratori di sistema)
X	Sono stati individuate, autorizzate ed istruite le risorse umane deputate al trattamento delle segnalazioni effettuate con modalità analogiche (RPCT, soggetti dal medesimo delegati ed amministratori di sistema)
N.A.	Sono stati individuati i Contitolari del trattamento ed è stato regolamentato il rapporto tra di essi
X	Sono stati individuati i Responsabili del trattamento ed è stato regolamentato il rapporto con il Titolare

Con particolare riferimento al **PERIMETRO DI CONOSCENZA** delle informazioni:

X	Sono stati verificati i presupposti per la comunicazione dei dati personali
N.A.	Sono stati verificati i presupposti per la diffusione dei dati personali
N.A.	Sono stati verificati i presupposti per il trasferimento dei dati personali extra UE (protezione equivalente)

Le segnalazioni sono sottratte all'**accesso** previsto dagli artt. 22 e ss. della Legge 7 agosto 1990, n. 241, e dagli artt. 5 e ss. del D.Lgs. 14 marzo 2013, n. 33 (articolo 12 del Decreto).
E' esclusa la **diffusione** del contenuto delle segnalazioni e dell'identità del segnalante o delle persone indicate come possibili responsabili delle condotte illecite o quelle a vario titolo coinvolte nelle vicende segnalate.

NON E' PREVISTO UN TRASFERIMENTO ALL'ESTERO, in quanto la piattaforma è installata presso il data center del Titolare.
Con particolare riferimento alla **progettazione, realizzazione ed utilizzo** dei canali di segnalazione interni:

X	il Titolare del trattamento adotta misure organizzative e tecniche volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione (privacy by design)
X	il Titolare del trattamento integra nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del presente regolamento e tutelare i diritti degli interessati (privacy by design)

X	Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento (privacy by default)

B.2.1.2. il trattamento rispetta i diritti degli interessati (CAPO III del Regolamento)

Questa sezione permette di dimostrare l'implementazione degli strumenti necessari per consentire agli interessati di esercitare i loro diritti.

In linea generale, tutti i diritti sanciti dal RGPD si applicano al trattamento dei dati personali tramite canali di segnalazione interni.

Sono previste le seguenti modalità di **informazione** dell'Interessato:

X	Su supporto cartaceo, a richiesta dell'Interessato
X	Su supporto cartaceo, in caso di incontro personale
N.A.	Su supporto cartaceo, all'interno della modulistica in uso agli uffici
N.A.	Elettronica
X	Sito web istituzionale
X	Cartellonistica esposta nei luoghi di lavoro
X	Richiamo all'interno degli atti di affidamento e contratti, in caso di rapporti con soggetti terzi rispetto al Titolare
N.A.	Messaggi audio/video
N.A.	Numero telefonico dedicato
N.A.	Comunicazione orale a cura dall'operatore

Rilevanza del **consenso** dell'Interessato

N.A.	Non necessario
X	Necessario in talune fattispecie (vedasi *supra*, in relazione alle basi giuridiche)
N.A.	Espresso in forma analogica
N.A.	Espresso in forma digitale

Possibilità di esercitare il diritto di **accesso**:

X	SI, mediante richiesta al RPCT in caso di utilizzo di modalità analogiche di presentazione della segnalazione
X	SI, mediante accesso alla piattaforma informatica
N.A.	NO

Possibilità di esercitare il diritto alla **rettifica**:

X	SI, mediante richiesta al RPCT in caso di utilizzo di modalità analogiche di presentazione della segnalazione
X	SI, mediante accesso alla piattaforma informatica
N.A.	NO

Possibilità di esercitare il diritto alla **integrazione**:

X	SI, mediante richiesta al RPCT in caso di utilizzo di modalità analogiche di presentazione della segnalazione
X	SI, mediante accesso alla piattaforma informatica
N.A.	NO

Possibilità di esercitare il diritto alla **cancellazione** (diritto all'oblio):

X	SI
N.A.	NO
X	NO, in relazione ai dati trattati per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento
X	NO, in relazione ai casi in cui non sia possibile individuare l'Interessato

Possibilità di esercitare il diritto alla **limitazione**:

X	SI, mediante richiesta al RPCT in caso di utilizzo di modalità analogiche di presentazione della segnalazione
X	SI, mediante accesso alla piattaforma informatica
N.A.	NO

Possibilità di esercitare il diritto alla **portabilità**:

X	NO
N.A.	SI, limitatamente ai dati raccolti sulla base del consenso

Possibilità di esercitare il diritto alla **opposizione**:

N.A	SI
X	NO, in quanto sussistono motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato
X	NO, in quanto il trattamento è necessario per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria

Diritto a non essere sottoposto ad un **processo decisionale automatizzato**:

X	in conseguenza dell'uso dei canali di segnalazione interni l'interessato non è sottoposto ad una decisione basata unicamente sul trattamento automatizzato, compresa la profilazione

La persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, non possono esercitare i diritti di cui sopra – per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata a garantire la riservatezza dell'identità del segnalante - secondo quanto previsto dall'articolo 2-undecies del D.Lgs. 30 giugno 2003, n. 196 (Codice privacy).

B.2.1.3. Il trattamento rispetta la normativa di settore, rilevante in tema di segnalazione di illeciti

Il Titolare del trattamento ha adempiuto agli obblighi ed alle prescrizioni contenute

X	Decreto Legislativo 10 marzo 2023, n. 24
X	Linee Guida ANAC approvate con Delibera n°311 del 12 luglio 2023

B.2.2. esito della verifica di conformità

Prima di procedere oltre con la Valutazione d'impatto, occorre constatare la conformità del trattamento sotto il profilo del rispetto alla normativa di protezione dei dati personali.
Conclusivamente, il trattamento si presenta:

X	**CONFORME** ALLA NORMATIVA DI PROTEZIONE DEI DATI PERSONALI e, pertanto, si può procedere con l'analisi che segue
N.A.	**NON CONFORME** ALLA NORMATIVA DI PROTEZIONE DEI DATI PERSONALI e, pertanto, si rende necessario sottoporlo ad ulteriore verifica

B.3. VALUTAZIONE DELLA OBBLIGATORIETÀ DELLA DPIA

Si rende a questo punto necessario verificare se l'esecuzione della presente DPIA sia resa necessaria in conseguenza di un obbligo normativo ovvero se essa sia svolta a seguito di una decisione discrezionale del Titolare del trattamento.

Dispone l'**articolo 13, comma 6 del Decreto** che "*soggetti di cui all'articolo 4 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, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*" .

C. MISURE DI SICUREZZA

In questa sezione sono riassunte le misure di sicurezza, **esistenti o pianificate** che contribuiscono alla sicurezza dei dati personali.

Esse sono ripartite in diverse categorie, sulla scorta della classificazione suggerita da **ENISA**. Per ciascuna categoria è altresì riportata la corrispondente categoria utilizzata dallo standard **ISO/IEC 27001:2013**.

INDICE DELLE MISURE		
ENISA		**ISO**
A. Politiche di sicurezza e procedure per la protezione dei dati personali		A.5 Politiche per la sicurezza delle informazioni
B. Ruoli e responsabilità		A.6.1.1 Ruoli e responsabilità per la sicurezza delle informazioni
C. Politica controllo accessi		A.9.1.1 Politica di controllo degli accessi
D. Gestione risorse e degli asset		A.8 Gestione degli asset
E. Change management		A.12.1 Procedure operative e responsabilità
F. Responsabile del trattamento (Data processors)		A.15 Relazione con i fornitori
G. Gestione degli incidenti / Violazione dei dati personali		A.16 Gestione degli incidenti relativi alla sicurezza delle informazioni
H. Business continuity		A.17 Aspetti relativi alla sicurezza delle informazioni nella gestione della continuità operativa
I. Riservatezza del personale		A.7 Sicurezza delle risorse umane
J. Formazione		A.7.2.2 Consapevolezza, istruzione, formazione e addestramento sulla sicurezza delle informazioni
K. Controllo accessi e autenticazione		A.9 Controllo degli accessi
L. Logging e monitoraggio		A.12.4 Raccolta dei log e monitoraggio
M. Sicurezza Server e Database		A.12 Sicurezza delle attività operative
O. Network/Communication security		A.13 Sicurezza delle comunicazioni
P. Backup		A.12.3 Backup
R. Sicurezza del ciclo di vita delle applicazioni		A.12.6 Gestione delle vulnerabilità tecniche A.14.2 Sicurezza nei processi di sviluppo e supporto
S. Cancellazione/eliminazione dei dati		A.8.3.2 Dismissione dei supporti A.11.2.7 Dismissione sicura o riutilizzo delle apparecchiature
T. Sicurezza fisica		A.11 Sicurezza fisica e ambientale

Si precisa che, con specifico riferimento al trattamento di dati personali mediante piattaforma informatica, il Responsabile del trattamento e/o gli altri responsabili (sub-responsabili), possiedono le seguenti certificazioni ovvero aderiscono ai seguenti Codici di condotta:

WHISTLEBLOWING SOLUTIONS I.S. S.R.L.,

X	UNI CEI EN ISO/IEC 27001:2017
X	QUALIFICAZIONE AGID/ACN
X	CSA CODE OF CONDUCT FOR GDPR COMPLIANCE (CSA STAR LEVEL 1)

SEEWEB SRL

X	ISO 27001:2013
X	ISO 22301:2019
X	ISO 27017:2015
X	ISO 27018:2014
X	ISO 20000-1:2018
X	ISO 9001:2015
X	CODICE DI CONDOTTA CISPE, RELATIVO ALLA TUTELA DEI DATI SUL CLOUD
X	CSA CODE OF CONDUCT FOR GDPR COMPLIANCE (CSA STAR LEVEL 1)
X	QUALIFICAZIONE AGID/ACN

La descrizione che segue riguarda le misure adottate:

a) dal Titolare del trattamento, in relazione sia alle segnalazioni ricevute mediante piattaforma informatica che mediante altro canale;
b) dal Responsabile (e/o altri responsabili) del trattamento, in relazione alle sole segnalazioni ricevute mediante la piattaforma informatica.

Con particolare riferimento al Responsabile (e/o altri responsabili) del trattamento, le misure di sicurezza di seguito riassunte devono intendersi come meramente riassuntive rispetto alla rilevazione delle misure effettuata a garanzia della conformità delle certificazioni dichiarate dai responsabili del trattamento, dagli organismi competenti.

A. Politiche di sicurezza e procedure per la protezione dei dati personali:

X	A.1 - L'organizzazione dovrebbe documentare la propria politica in merito all'elaborazione dei dati personali come parte della sua politica di sicurezza delle informazioni
X	A.2 - La politica di sicurezza dovrebbe essere riesaminata e aggiornata, se necessario, su base annuale
X	A.3 - L'organizzazione dovrebbe documentare una politica di sicurezza dedicata separata per quanto riguarda il trattamento dei dati personali. La politica dovrebbe essere approvata dalla Direzione e comunicata a tutti i dipendenti e alle parti esterne interessate
X	A.4 - La politica di sicurezza dovrebbe almeno fare riferimento a: i ruoli e le responsabilità del personale, le misure tecniche e organizzative di base adottate per la sicurezza dei dati personali, per i responsabili del trattamento dei dati o per le altre terze parti coinvolte nel trattamento dei dati personali
N.A.	A.5 - Dovrebbe essere creato e mantenuto un inventario di politiche / procedure specifiche relative alla sicurezza dei dati personali, basato sulla politica generale di sicurezza
N.A.	A.6 - La politica di sicurezza dovrebbe essere riesaminata e aggiornata, se necessario, su base semestrale

Misure specifiche adottate dal Titolare:

X	Adozione di un Modello Organizzativo in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati
X	Valutazione di fattispecie di contitolarità del trattamento
X	Adozione di istruzioni specifiche in capo ai soggetti autorizzati al trattamento in questione
X	Adozione di istruzioni generali in tema di protezione dei dati personali
X	Le autorizzazioni al trattamento (e le relative autenticazioni) sono riconosciute in quanto necessarie allo svolgimento dei compiti e delle mansioni assegnate al personale
X	Le autorizzazioni al trattamento (e le relative autenticazioni) sono riconosciute ed assegnate con scadenza temporale, soggetta a revisione periodica
X	Adozione di politiche specifiche per gli Amministratori di sistema

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

B. Ruoli e responsabilità:

X	B.1 - I ruoli e le responsabilità relativi al trattamento dei dati personali devono essere chiaramente definiti e assegnati in conformità con la politica di sicurezza
X	B.2 - Durante le riorganizzazioni interne o le cessazioni e il cambio di impiego, devono essere chiaramente definite le modalità di revoca dei diritti e delle responsabilità con le rispettive procedure di passaggio di consegne
X	B.3 - Dovrebbe essere effettuata una chiara individuazione e designazione delle persone incaricate di compiti specifici di sicurezza, compresa la nomina di un responsabile della sicurezza
X	B.4 - Il responsabile della sicurezza dovrebbe essere nominato formalmente (in modo documentato). Anche i compiti e le responsabilità del responsabile della sicurezza dovrebbero essere chiaramente definiti e documentati
X	B.5 - Doveri e aree di responsabilità che possono essere in conflitto, ad esempio i ruoli di responsabile della sicurezza, auditor e DPO, dovrebbero essere considerati separati per ridurre le opportunità di modifiche non autorizzate o non intenzionali o di uso improprio di dati personali

Misure specifiche adottate dal Titolare:

X	Il soggetto Responsabile della gestione dei canali di segnalazione interni è il Responsabile della Prevenzione della corruzione e della trasparenza (RPCT)
X	Previsione della figura di "Custode delle identità" nella gestione delle segnalazioni effettuate mediante piattaforma informatica

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

C. Politica controllo accessi:

X	C.1 - I diritti specifici di controllo dell'accesso dovrebbero essere assegnati a ciascun ruolo (coinvolto nel trattamento di dati personali) in base al principio di necessità e di pertinenza
X	C.2 - Una politica di controllo degli accessi dovrebbe essere dettagliata e documentata. L'organizzazione dovrebbe determinare in questo documento le regole di controllo di accesso appropriate, i diritti di accesso e le restrizioni per specifici ruoli degli utenti verso i processi e le procedure relative ai dati personali
X	C.3 - La segregazione dei ruoli per gestire il controllo degli accessi (ad es. Richiesta di accesso, autorizzazione di accesso, amministrazione degli accessi) dovrebbe essere chiaramente definita e documentata
X	C.4 - I ruoli con diritti di accesso privilegiato dovrebbero essere chiaramente definiti e assegnati limitatamente a membri specifici del personale

Misure specifiche adottate dal Titolare:

X	Gli accessi del RPCT e degli operatori autorizzati ad operare sulla piattaforma avvengono mediante procedure di autenticazione personale

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

D. Gestione risorse e degli asset:

X	D.1 - L'organizzazione dovrebbe disporre di un registro delle risorse IT utilizzate per il trattamento dei dati personali (hardware, software e rete). Il registro potrebbe includere almeno le seguenti informazioni: risorsa IT, tipo (ad es. server, workstation), posizione (fisica o elettronica). Ad una persona specifica dovrebbe essere assegnato il compito di mantenere e aggiornare il registro (ad esempio, il responsabile IT)
X	D.2 - Le risorse IT dovrebbero essere riesaminate e aggiornate regolarmente
X	D.3 - I ruoli che hanno accesso a determinate risorse dovrebbero essere definiti e documentati
N.A.	D.4 - Le risorse IT dovrebbero essere riesaminate e aggiornate su base annuale

Misure specifiche adottate dal Titolare:

X	Il software installato per la gestione della piattaforma è fornito dalla società Whistleblowing Solutions in modalità SaaS
X	La piattaforma è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto

X	Il Responsabile tiene costantemente aggiornato il software sulla base dei rilasci effettuati dal produttore
X	Il software è stato sviluppato in compliance con ISO 37002 and EU Directive 2019/1937
X	E' previsto il supporto nativo per https nella versione TLS 1.2+
X	Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents
X	Il software utilizzato per la realizzazione della piattaforma è conforme agli standard per la sicurezza delle applicazioni (OWASP)
X	Nessun dato viene esposto o trasferito al di fuori della piattaforma

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

E. Gestione delle modifiche:

X	E.1 - L'organizzazione deve assicurarsi che tutte le modifiche al sistema IT siano registrate e monitorate da una persona specifica (ad esempio, responsabile IT o sicurezza). Questo processo dovrebbe essere monitorato regolarmente
X	E.2 - Lo sviluppo del software dovrebbe essere eseguito in un ambiente speciale, non collegato al sistema IT utilizzato per il trattamento dei dati personali. Quando è necessario eseguire l test, devono essere utilizzati dati fittizi (non dati reali). Nei casi in cui ciò non è possibile, dovrebbero essere previste procedure specifiche per la protezione dei dati personali utilizzati nei test
X	E.3 - Dovrebbe essere presente una politica dettagliata e documentata di gestione dei cambiamenti. Dovrebbe includere: un processo per l'introduzione dei cambiamenti, i ruoli / utenti che hanno i diritti di cambiamento, le tempistiche per l'introduzione dei cambiamenti. La politica di gestione dei cambiamenti dovrebbe essere regolarmente aggiornata

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	Il Responsabile tiene costantemente aggiornato il software sulla base dei rilasci effettuati dal produttore
X	Gli interventi di manutenzione/assistenza sulle componenti hardware e software del sistema avvengono da parte del personale del Responsabile

F. Responsabile del trattamento (Data processor):

X	F.1 - Le linee guida e le procedure formali relative al trattamento dei dati personali da parte dei responsabili del trattamento dei dati (appaltatori / outsourcer) dovrebbero essere definite, documentate e concordate tra il titolare del trattamento e il responsabile del trattamento prima dell'inizio delle attività di trattamento. Queste linee guida e procedure dovrebbero stabilire obbligatoriamente lo stesso livello di sicurezza dei dati personali come richiesto nella politica di sicurezza dell'organizzazione
X	F.2 - E' necessario predisporre clausole contrattuali per le quali al rilevamento di una violazione dei dati personali, il responsabile del trattamento informi il titolare del trattamento senza indebiti ritardi

X	F.3 - Fra il titolare del trattamento dei dati e il responsabile del trattamento dei dati dovrebbero essere formalmente concordati requisiti formali e obblighi. Il Responsabile del trattamento dovrebbe fornire prove documentate sufficienti di conformità
X	F.4 - L'organizzazione Titolare del trattamento dei dati dovrebbe verificare regolarmente la conformità del Responsabile del trattamento al livello concordato di requisiti e obblighi
X	F.5 - Il personale del responsabile del trattamento che elabora dati personali deve essere soggetto a specifici accordi documentati di riservatezza / non divulgazione

Misure specifiche adottate dal Titolare:

X	Titolare e Responsabile del trattamento hanno sottoscritto un accordo sul trattamento dei dati personali ai sensi dell'art. 28 RGPD
X	Il trattamento dei dati personali da parte del Responsabile è limitato al periodo di vigenza del servizio affidato
X	In caso di cessazione del rapporto con il Responsabile i dati presenti sulla piattaforma informatica sono cancellati entro i 15 giorni successivi

G. Gestione degli incidenti / violazione dei dati personali (documento "Policy Gestione incidenti di sicurezza")

X	G.1 - È necessario definire un piano di risposta agli incidenti con procedure dettagliate per garantire una risposta efficace e ordinata agli incidenti relativi ai dati personali
X	G.2 - Le violazioni dei dati personali devono essere segnalate immediatamente alla Direzione. Dovrebbero essere in atto procedure di notifica per la segnalazione delle violazioni alle autorità competenti e agli interessati, ai sensi dell'art. 33 e 34 GDPR
X	G.3 - Il piano di risposta degli incidenti dovrebbe essere documentato, compreso un elenco di possibili azioni di mitigazione e una chiara assegnazione dei ruoli
X	G.4 - Gli incidenti e le violazioni dei dati personali devono essere registrati insieme ai dettagli riguardanti l'evento e le successive azioni di mitigazione eseguite

Misure specifiche adottate dal Titolare:

X	Adozione di una Data Breach Policy
X	Assegnazione compiti e responsabilità specifiche
X	Previsione di specifici obblighi per Contitolari/Responsabili
X	Previsione di una formazione specifica per il personale in materia di sicurezza e violazione di dati personali
X	Istituzione di un registro delle violazioni di dati personali
X	Istituzione di un registro degli incidenti non costituenti violazioni di dati personali

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	Definita una procedura per la gestione delle violazioni dei dati personali

H. Business continuity:

X	H.1 - L'organizzazione dovrebbe stabilire le procedure e i controlli principali da seguire al fine di garantire il livello richiesto di continuità e disponibilità del sistema informatico che elabora i dati personali (in caso di incidente / violazione dei dati personali)
X	H.2 - Un BCP dovrebbe essere dettagliato e documentato (seguendo la politica generale di sicurezza). Dovrebbe includere azioni chiare e assegnazione di ruoli
X	H.3 - Un livello di qualità del servizio garantito dovrebbe essere definito nel BCP per i processi aziendali fondamentali che prevedono la sicurezza dei dati personali
X	H.4 - Deve essere nominato personale specifico con la necessaria responsabilità, autorità e competenza per gestire la continuità operativa in caso di incidente / violazione dei dati personali
X	H.5 - Si dovrebbe prendere in considerazione una struttura alternativa, a seconda dell'organizzazione e dei tempi di inattività accettabili del sistema IT

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

I. Riservatezza del personale:

X	I.1 - L'organizzazione dovrebbe garantire che tutto il personale comprenda le proprie responsabilità e gli obblighi relativi al trattamento dei dati personali. I ruoli e le responsabilità devono essere chiaramente comunicati durante il processo di pre-assunzione e / o inserimento
X	I.2 - Prima di assumere i propri compiti, il personale dovrebbe essere invitato a riesaminare e concordare la politica di sicurezza dell'organizzazione e firmare i rispettivi accordi di riservatezza e di non divulgazione
X	I.3 - Il personale coinvolto nel trattamento dei dati personali ad alto rischio dovrebbe essere vincolato a specifiche clausole di riservatezza (ai sensi del contratto di lavoro o altro atto legale)

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

J. Formazione del personale:

X	J.1 - L'organizzazione dovrebbe garantire che tutto il personale sia adeguatamente informato sui controlli di sicurezza del sistema informatico relativi al suo lavoro quotidiano. Il personale coinvolto nel trattamento dei dati personali dovrebbe inoltre essere adeguatamente informato in merito ai requisiti in materia di protezione dei dati e agli obblighi legali attraverso regolari campagne di sensibilizzazione
X	J.2 - L'organizzazione dovrebbe disporre di programmi di formazione strutturati e regolari per il personale, compresi i programmi specifici (relativi alla protezione dei dati personali) per l'inserimento dei nuovi arrivati
X	J.3 - Un piano di formazione con obiettivi e obiettivi definiti dovrebbe essere preparato ed eseguito su base annuale

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

K. Controllo accessi IT e autenticazione:

X	K.1 - Dovrebbe essere attuato un sistema di controllo accessi applicabile a tutti gli utenti che accedono al sistema IT. Il sistema dovrebbe consentire la creazione, l'approvazione, il riesame e l'eliminazione degli account degli utenti
X	K.2 - L'uso di account generici (non personali) dovrebbe essere evitato. Nei casi in cui ciò è necessario, è necessario garantire che tutti gli utenti che usano l'account generico abbiano gli stessi ruoli e responsabilità
X	K.3 - Dovrebbe essere presente un meccanismo di autenticazione che consenta l'accesso al sistema IT (basato sulla politica e sul sistema di controllo degli accessi). Come minimo deve essere utilizzata una combinazione di user-id e password. Le password dovrebbero rispettare un certo livello (configurabile) di complessità
X	K.4 - Il sistema di controllo degli accessi dovrebbe essere in grado di rilevare e non consentire l'utilizzo di password che non rispettano un certo livello di complessità (configurabile)
X	K.5 - Una politica specifica per la password dovrebbe essere definita e documentata. La politica deve includere almeno la lunghezza della password, la complessità, il periodo di validità e il numero di tentativi di accesso non riusciti accettabili
N.A.	K.6 - Le password degli utenti devono essere archiviate in formato "hash"
X	K7 - L'autenticazione a due fattori dovrebbe preferibilmente essere utilizzata per accedere ai sistemi che elaborano i dati personali. I fattori di autenticazione potrebbero essere password, token di sicurezza, chiavette USB con token segreto, dati biometrici, ecc.
N.A.	K.8 - Dovrebbe essere utilizzata l'autenticazione dei dispositivi per garantire che l'elaborazione dei dati personali venga eseguita solo attraverso risorse di rete specifiche

Misure specifiche adottate dal Titolare:

X	Il titolare verifica costantemente i diritti di accesso degli utenti; le credenziali sono disattivate in caso di perdita della qualità che consente all'utente l'accesso ai dati
X	Il personale è istruito in relazione alla creazione ed all'uso di password sicure
X	L'operatore è adeguatamente edotto sulla necessità di bloccare lo schermo in caso di allontanamento dalla postazione

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.
X	Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password
X	Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238

L. Logging e monitoraggio:

X	L.1 - I log devono essere attivati per ogni sistema / applicazione utilizzata per il trattamento dei dati personali. Dovrebbero includere tutti i tipi di accesso ai dati (visualizzazione, modifica, cancellazione)

N.A.	L.2 - I log devono essere registrati con marcatura temporale (timestamp) e adeguatamente protetti da manomissioni e accessi non autorizzati. Gli orologi dovrebbero essere sincronizzati con un'unica fonte temporale di riferimento
X	L.3 - È necessario registrare le azioni degli amministratori di sistema e degli operatori di sistema, inclusa l'aggiunta / eliminazione / modifica dei diritti di accesso degli utenti
X	L.4 - Non dovrebbe esserci alcuna possibilità di cancellazione o modifica del contenuto dei log. Anche l'accesso ai log deve essere registrato oltre al monitoraggio per rilevare attività insolite
N.A.	L.5 - Un sistema di monitoraggio dovrebbe elaborare i log e produrre rapporti sullo stato del sistema e notificare potenziali allarmi

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	L'applicativo GlobaLeaks 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
X	I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent
X	I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

M. Sicurezza Server e Database:

N.A.	M.1 - I database e application server devono essere configurati affinché lavorino con un account separato, con i privilegi minimi del sistema operativo per funzionare correttamente
N.A.	M.2 - I database e application server devono elaborare solo i dati personali che sono effettivamente necessari per l'elaborazione al fine di raggiungere i propri scopi di elaborazione
X	M.3 - Le soluzioni di crittografia dovrebbero essere considerate su specifici file o record attraverso l'uso di software o hardware
X	M.4 - È necessario prendere in considerazione la crittografia delle unità di archiviazione
N.A.	M.5 - Le tecniche di pseudonimizzazione dovrebbero essere applicate attraverso la separazione dei dati dagli identificatori diretti per evitare il collegamento all'interessato senza ulteriori informazioni
N.A.	M.6 - Dovrebbero essere considerate le tecniche che supportano la privacy a livello di database, come le authorized queries, il privacy preserving data base querying, la searchable encryption, ecc.

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	Il contenuto delle segnalazioni e l'identità del segnalante sono crittografati
X	Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.
X	Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto

X	Tutti i computer del personale del Responsabile e dei sub-responsabili eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware

N. Network/Communication security:

X	O.1 - Ogni volta che l'accesso viene eseguito tramite Internet, la comunicazione deve essere crittografata tramite protocolli crittografici (TLS / SSL)
N.A.	O.2 - L'accesso wireless al sistema IT dovrebbe essere consentito solo a utenti e processi specifici. Dovrebbe essere protetto da meccanismi di crittografia
X	O.3 - In generale, l'accesso remoto al sistema IT dovrebbe essere evitato. Nei casi in cui ciò sia assolutamente necessario, dovrebbe essere eseguito solo sotto il controllo e il monitoraggio di una persona specifica dall'organizzazione (ad esempio amministratore IT / responsabile della sicurezza) attraverso dispositivi predefiniti
X	O.4 - Il traffico da e verso il sistema IT deve essere monitorato e controllato tramite firewall e sistemi di rilevamento delle intrusioni
N.A.	O.5 - La connessione a Internet non dovrebbe essere consentita ai server e alle workstation utilizzate per il trattamento dei dati personali
N.A.	O.6 - La rete IT dovrebbe essere separata dalle altre reti del titolare
N.A.	O.7 - L'accesso al sistema IT deve essere eseguito solo da dispositivi e terminali preautorizzati utilizzando tecniche come il MAC filtering o il Network Access Control (NAC)

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	La piattaforma informatica dispone di un supporto nativo per https nella versione TLS 1.2+

O. Backup:

X	P.1 - Le procedure di backup e ripristino dei dati devono essere definite, documentate e chiaramente collegate a ruoli e responsabilità
X	P.2 - Ai backup dovrebbe essere assegnato un livello adeguato di protezione fisica e ambientale coerente con gli standard applicati sui dati di origine
X	P.3 - L'esecuzione dei backup deve essere monitorata per garantire la completezza
X	P.4 - I backup completi devono essere eseguiti regolarmente
X	P.5 - I supporti di backup dovrebbero essere testati regolarmente per assicurarsi che possano essere utilizzati
X	P.6 - I backup incrementali programmati dovrebbero essere eseguiti almeno su base giornaliera
X	P.7 - Le copie del backup devono essere conservate in modo sicuro in luoghi diversi dai dati di origine
X	P.8 - Se viene utilizzato un servizio di terze parti per l'archiviazione di backup, la copia deve essere crittografata prima di essere trasmessa dal titolare dei dati

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery

P. Sicurezza del ciclo di vita delle applicazioni:

X	R.1 - Durante il ciclo di vita dello sviluppo si devono seguire le migliori pratiche, lo stato dell'arte e pratiche, framework o standard di sicurezza ben noti
X	R.2 - Specifici requisiti di sicurezza dovrebbero essere definiti durante le prime fasi del ciclo di vita dello sviluppo
X	R.3 - Le tecnologie e le tecniche specifiche progettate per supportare la privacy e la protezione dei dati (denominate anche tecnologie di miglioramento della privacy (PET Privacy Enhancing Technologies)) dovrebbero essere adottate in analogia con i requisiti di sicurezza
X	R.4 - Dovrebbero essere seguiti standard e pratiche di codifica sicure
X	R.5 - Durante lo sviluppo, devono essere eseguiti test e convalida rispetto all'implementazione dei requisiti di sicurezza iniziali
X	R.6 - I vulnerability assessment, i penetration test applicativi e dell'infrastruttura dovrebbero essere eseguiti da una terza parte fidata prima del passaggio in ambiente di produzione. Il passaggio non può avvenire a meno che non sia raggiunto il livello di sicurezza richiesto
N.A.	R.7 - Devono essere eseguiti penetration test periodici
N.A.	R.8 - Si dovrebbero ottenere informazioni sulle vulnerabilità tecniche dei sistemi IT utilizzati
N.A.	R.9 - Le patch software dovrebbero essere testate e valutate prima di essere installate in ambiente di produzione

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Q. Cancellazione/eliminazione dei dati:

X	S.1 - Software di sovrascrittura dovrebbe essere usato su tutti i supporti prima della loro eliminazione. Nei casi in cui ciò non è possibile (CD, DVD, ecc.), i supporti dovrebbero essere distrutti fisicamente
X	S.2 - È necessario eseguire la triturazione di carta e supporti portatili utilizzati per memorizzare i dati personali
X	S.3 - Più passaggi di software di sovrascrittura devono essere eseguiti su tutti i supporti prima di essere smaltiti
X	S.4 - Se i servizi di terzi sono utilizzati per eliminare in modo sicuro i supporti o i documenti cartacei, è necessario stipulare un contratto di servizio e produrre un attestato di distruzione, a seconda dei casi
X	S.5 - Dopo la cancellazione dei dati con un software, devono essere eseguite misure hardware aggiuntive quali la smagnetizzazione. A seconda dei casi, dovrebbe essere considerata anche la distruzione fisica
N.A.	S.6 - Se una terza parte, quindi un responsabile del trattamento, viene utilizzata per la distruzione di supporti o documenti cartacei, il processo si potrebbe svolgere presso le sedi del titolare del trattamento (ed evitare il trasferimento dei dati personali

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

R. Sicurezza fisica:

X	T.1 - Il perimetro fisico dell'infrastruttura IT non dovrebbe essere accessibile da personale non autorizzato

X	T.2 - L'identificazione chiara, tramite mezzi appropriati, ad es. badge identificativi, per tutto il personale e i visitatori che accedono ai locali dell'organizzazione, dovrebbe essere stabilita, a seconda dei casi
X	T.3 - Le zone sicure dovrebbero essere definite e protette da appropriati controlli di accesso. Un registro fisico o una traccia elettronica di controllo di tutti gli accessi devono essere mantenuti e monitorati in modo sicuro
X	T.4 - I sistemi di rilevamento antintrusione dovrebbero essere installati in tutte le zone di sicurezza
X	T.5 - Le barriere fisiche dovrebbero, se del caso, essere costruite per impedire l'accesso fisico non autorizzato
X	T.6 - Le aree non usate dovrebbero essere fisicamente bloccate e periodicamente riesaminate
X	T.7 - Un sistema antincendio automatico, un sistema di climatizzazione dedicato e chiuso e un gruppo di continuità (UPS) dovrebbero essere usati nella sala server
X	T.8 - Il personale di supporto esterno deve avere accesso limitato alle aree protette

Con specifico riferimento alla piattaforma informatica, il livello di implementazione è quello risultante dalle certificazioni in possesso di Responsabile e sub-responsabili del trattamento.

Misure specifiche adottate dal Responsabile:

X	I datacenter del fornitore IaaS 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
X	I datacenter del fornitore IaaS sono certificati ISO27001

D. Esecuzione della Valutazione d'Impatto sulla Protezione dei Dati Personali (DPIA)

Il trattamento dei dati personali è un'attività che espone a rischio gli interessati, ossia le persone fisiche cui i dati si riferiscono.

I rischi per i diritti e le libertà delle persone fisiche possono derivare dal fatto che il trattamento, in ragione delle caratteristiche sue proprie, possa cagionare danni materiali e immateriali, come per esempio, discriminazioni, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale significativo (**Considerando 75 del RGPD**).

Posto che, sulla scorta delle considerazioni esposte nel paragrafo che precede, il trattamento in questione presenta "naturalmente" un rischio per i diritti e le libertà delle persone fisiche, la normativa di protezione richiede al Titolare del trattamento l'adozione di misure adeguate a gestire e limitare tale rischio.

Le attività di valutazione d'impatto sulla protezione dei dati personali (DPIA) sono finalizzate, prioritariamente, a contenere la probabilità e l'impatto che eventuali violazioni di dati personali (denominate nell'accezione inglese "data breach") potrebbero comportare sulle persone fisiche alle quali i dati si riferiscono.

Lo scopo è stabilire se e fino a che punto un'attività di trattamento, per le sue caratteristiche, il tipo di dati cui si riferisce o il tipo di operazioni svolte possa causare danni alle parti interessate e quali siano le misure disponibili per contenere il rischio (per esempio, la cifratura dei dati e la pseudonimizzazione, i test di sicurezza, i sistemi di continuità operative e le procedure di backup).

D.1. Analisi dei possibili impatti e loro gravità

Si cerca di determinare un reale e potenziale impatto sui diritti e le libertà degli interessati, **tenendo in considerazione i controlli e le contromisure esistenti**, pianificate o implementate al fine di ridurre tale rischio, utilizzando una scala di valori (basso, medio, alto, molto alto).

La valutazione tiene conto delle differenti ipotesi di danno (fisici, materiali o morali). A seconda delle circostanze, una violazione può riguardare tutti gli aspetti sottoindicati od una combinazione di essi.

Il livello di rischio può aumentare o diminuire considerando i seguenti fattori:
- natura, carattere sensibile e volume de dati personali trattati;
- livello di identificazione dei dati;
- natura della fonte del rischio;
- numero di interconnessioni (interessati, parti terze, stati esteri, …);
- numero e tipologia di dispositivi informatici impiegati.

Scala di misurazione dell'impatto (suggerita da ENISA)

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
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.)
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.)
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.)

Le **minacce alla sicurezza** dei dati personali possono essere classificate, avendo riguardo al tipo di violazione dei dati personali che possono determinare, in:

violazione della riservatezza	in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
violazione dell'integrità	in caso di modifica non autorizzata o accidentale dei dati personali
violazione della disponibilità	in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

Questa scala di misurazione viene utilizzata per valutare, separatamente, l'impatto sulle persone fisiche derivante dalla violazione di riservatezza, integrità e disponibilità dei dati.

D.1.1. Perdita di riservatezza (Confidentiality Breach)

La perdita di confidenzialità o riservatezza consegue tipicamente a due violazioni: la divulgazione e l'accesso. Occorre determinare quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti attraverso i canali di segnalazione interni fossero oggetto di accesso ad opera di terzi non aventi diritto.

Con il termine "**divulgazione**" si intendono una comunicazione o diffusione non autorizzate od improprie dei dati personali, non corrispondenti ad informazioni di pubblico dominio, verso terze parti, anche se non note o identificabili. In alcuni casi la divulgazione può seguire un accesso ai dati da parte di soggetti non aventi diritto; in altri casi può essere dovuta a trattamenti non conformi di dati personali.

Con il termine "**accesso**" si intende l'accesso (anche in sola visualizzazione) ai dati trattati dal Titolare da parte di soggetti non aventi diritto al momento della violazione.
L'accesso ai dati non implica che si sia verificata anche un'altra violazione, quale la distruzione, l'alterazione o la divulgazione: il soggetto non avente diritto potrebbe utilizzare a proprio favore le informazioni ricavabili dai dati senza distruggerli, alterarli o divulgarli.

Occorre in ogni caso verificare se le misure di sicurezza (es.: cifratura dei dati) in uso rendano improbabile l'identificazione degli interessati (non compromissione della chiave, algoritmo di cifratura o impronta senza vulnerabilità note).
(Ad esempio, un documento cartaceo o un laptop contenente dati personali viene perso durante il trasporto; l'attrezzatura è stata smaltita senza distruzione dei dati personali; i dati personali vengono inviati erroneamente a una serie di destinatari non autorizzati; alcuni utenti potrebbero accedere agli account di altri utenti in un servizio online; i dati personali sono pubblicati su una bacheca Internet o su un sito p2p; un CD-ROM con i dati del cliente è stato rubato dai locali in cui era conservato, un sito web configurato in modo errato rende pubblicamente accessibili su internet i dati degli utenti interni).

Possibili conseguenze che una divulgazione non autorizzata (perdita di riservatezza) di dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato:

X	I dati potrebbero essere divulgati al di fuori di quanto previsto dall'informativa ovvero dalla disciplina di riferimento
X	I dati potrebbero essere oggetto di accesso da parte di soggetti non aventi diritto al momento della violazione
X	I dati potrebbero essere correlati, senza sforzo irragionevole, ad altre informazioni relative agli interessati
X	I dati potrebbero essere utilizzati per finalità diverse da quelle previste oppure in modo non lecito

Potenziale Impatto che una divulgazione non autorizzata (perdita di riservatezza) di dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato:

X	Ritorsione, intesa come qualsiasi comportamento, atto od omissione, anche solo tentato o minacciato, posto in essere in ragione della segnalazione e che provoca o può provocare alla persona segnalante, in via diretta o indiretta, un danno ingiusto
X	Perdita del controllo dei dati personali
X	Limitazione dei diritti
X	Discriminazione
X	Furto o usurpazione di identità
N.A.	Frodi
N.A.	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
X	Pregiudizio alla reputazione

X	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
X	Conoscenza da parte di terzi non autorizzati
N.A.	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che una divulgazione non autorizzata (**perdita di riservatezza**) di dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato:

La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	GRAVITA' IMPATTO
DATI COMUNI	**ALTO**
DATI SENSIBILI (ART. 9 RGPD)	**ALTO**
DATI GIUDIZIARI (ART. 10 RGPD)	**ALTO**

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di canali di segnalazione interni, l'impatto complessivo della perdita di riservatezza è da considerarsi **ALTO**, anche in considerazione dell'esistenza di una specifica normativa di tutela apprestata dal legislatore nazionale e comunitario.

D.1.2. Perdita di integrità (Integrity Breach)

Determinazione di quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti attraverso i canali di segnalazione interni fossero oggetto di un'**alterazione non autorizzata**.

La "alterazione" è la situazione in cui **i dati sono danneggiati, corrotti o non più completi**. L'alterazione non autorizzata può essere la conseguenza di un attacco esterno o di una manipolazione inconsapevole da parte di personale non competente. Un'alterazione accidentale si può verificare per errore umano (ad es. nel momento di un aggiornamento delle informazioni) o per un disguido tecnico quando all'interno di una base dati si perdono i collegamenti a determinate informazioni (integrità referenziale).

L'alterazione non autorizzata dei dati può comportare:
- la comunicazione di informazioni erronee a soggetti esterni alla struttura del Titolare o alpubblico;
- errori nel trattamento o trattamento non conforme;
- decisioni errate con effetti sull'interessato.

In alcuni casi l'alterazione può seguire un accesso ai dati da parte di soggetti non aventi diritto; in altri casi può essere dovuta ad errori nel trattamento.

Occorre comunque verificare se sia possibile il recupero degli stessi in tempi compatibili con i diritti degli interessati.
(Ad esempio, è stato modificato un record necessario per la fornitura di un servizio sociale online e l'individuo deve richiedere il servizio in modalità offline; è stato modificato un record importante per l'accuratezza del file di un individuo in un servizio medico online).

Possibili conseguenze che un'alterazione non autorizzata (**perdita di integrità**) dei dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato

X	I dati potrebbero essere modificati e resi inconsistenti
X	I dati potrebbero essere modificati mantenendo la consistenza
X	Potrebbero essere comunicate informazioni erronee a soggetti esterni alla struttura del Titolare o al pubblico
X	Potrebbero esservi errori nel trattamento o verificarsi un trattamento non conforme
X	Potrebbero essere assunte decisioni errate con effetti sull'interessato

Potenziale Impatto che un'alterazione non autorizzata (**perdita di integrità**) di dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato

X	Perdita del controllo dei dati personali
X	Limitazione dei diritti
X	Discriminazione
X	Furto o usurpazione di identità
N.A.	Frodi
X	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
X	Pregiudizio alla reputazione
N.A.	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
N.A.	Conoscenza da parte di terzi non autorizzati
X	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che un'alterazione non autorizzata (**perdita di integrità**) dei dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato:

La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	GRAVITA' IMPATTO
DATI COMUNI	**ALTO**
DATI SENSIBILI (ART. 9 RGPD)	**ALTO**
DATI GIUDIZIARI (ART. 10 RGPD)	**ALTO**

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di canali di segnalazione interni, l'impatto complessivo della perdita di integrità è da considerarsi **ALTO**, in considerazione del fatto che il contenuto delle segnalazioni e dei documenti eventualmente prodotti dal segnalante può determinare l'assunzione di provvedimenti (disciplinari e giudiziari) ad elevato impatto sui diritti e le libertà del segnalante e delle persone indicate come possibili responsabili delle condotte illecite o di quelle a vario titolo coinvolte nelle vicende segnalate.

D.1.3. Perdita di disponibilità (Availability Breach)

Determinazione di quale potrebbe essere l'impatto sull'Interessato nel caso in cui i dati raccolti attraverso i canali di segnalazione interni fossero oggetto di una distruzione non autorizzata o perdita.

Con il termine "**indisponibilità**" si intende la indisponibilità, irreversibile o temporanea, dei mezzi e degli strumenti necessari per effettuare il trattamento dei dati da parte degli Interessati o del Titolare per l'erogazione di servizi richiesti o per conto dell'Interessato.
L'indisponibilità non implica la distruzione dei dati personali.
L'indisponibilità irreversibile di un mezzo o strumento, richiede l'adozione di nuovi mezzi o strumenti per accedere ai dati.
Tale violazione può essere relativa a:
- indisponibilità dei sistemi e dei servizi informatici mediante i quali le informazioni sono accessibili (ad es. in caso di attacco informatico);
- indisponibilità di mezzi e strumenti necessari per l'accesso alle informazioni (ad es. perdita di una chiave di decifratura o di un token hardware di accesso con la possibilità di accedere ai dati in backup o altri archivi);
- indisponibilità degli strumenti atti ad identificare l'informazione all'interno di grandi archivi cartacei od elettronici;
- degrado prestazionale dei servizi informatici che determina l'impossibilità di perfezionare operazioni di trattamento;
- modifiche tecnologiche che rendono impossibile la decodifica dei dati rappresentati secondo particolari formati di memorizzazione.

Con il termine "**perdita**" si intende la perdita del supporto fisico di memorizzazione dei dati (ad es. privazione, sottrazione, smarrimento dei dispositivi contenenti i dati oppure dei documenti cartacei). La perdita di dati è la situazione in cui i dati, presumibilmente, esistono ancora, ma il Titolare ne ha perso il controllo o la possibilità di accedervi.
La perdita di un supporto fisico di memorizzazione dei dati non implica che si sia verificata anche un'altra violazione quale la distruzione, l'indisponibilità, l'accesso o la divulgazione (ad es., un disco DVD perso può contenere una copia cifrata dei dati).

Con il termine "**distruzione**" si intende la indisponibilità irreversibile o di lunga durata di dati personali trattati dal Titolare. La distruzione dei dati personali è la condizione in cui i dati non esistono più o non esistono più in un formato che sia utilizzabile dal Titolare.
La violazione può essere relativa a:
- eliminazione logica non autorizzata (ad es., cancellazione dei dati);
- eliminazione fisica (ad es., danneggiamento o distruzione dei supporti di memorizzazione o dei documenti cartacei);
- eliminazione logica o fisica dei dati in formato elettronico, il cui ripristino da documenti cartacei è possibile ma con un impiego di tempo elevato, tale da poter generare effetti sull'interessato.

In questo scenario, i dati personali possono essere recuperati solo:
* direttamente dall'Interessato;
* da fonti esterne quali fonti pubbliche e/o di terze parti;
* da archivi cartacei (in caso di distruzione, il recupero da tali archivi si suppone estremamente complesso, di lunga durata e con il rischio di ottenere dati non aggiornati).

Ci sarà sempre una violazione della Disponibilità del dato nel caso di perdita o distruzione permanente dei dati. L'indisponibilità dei dati è quindi da considerare una violazione quando potrebbe avere un impatto significativo sui diritti e le libertà delle persone fisiche. Non si tratta invece di una violazione quando l'indisponibilità è dovuta a interruzioni programmate per la manutenzione.

(Ad esempio, un database di utenti è danneggiato ed è necessaria un'attività gravosa per riportare il servizio in linea; un file personale viene perso e l'individuo deve fornire nuovamente alcune informazioni all'Ente; un file è stato perso/il database è danneggiato e non è stato eseguito il backup di queste informazioni; un servizio critico (ad es. cartella clinica online) è inattivo e non può essere recuperato immediatamente)

Possibili conseguenze che una distruzione non autorizzata (**perdita di disponibilità**) dei dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato

X	Mancato accesso a servizi
X	Malfunzionamento e difficoltà nell'utilizzo di servizi
N.A.	Impossibilità di decodifica dei dati rappresentati secondo particolari formati di memorizzazione
X	Mancato accesso alle informazioni

Potenziale Impatto che una distruzione non autorizzata (**perdita di disponibilità**) di dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato:

X	Perdita del controllo dei dati personali
X	Limitazione dei diritti
N.A.	Discriminazione
N.A.	Furto o usurpazione di identità
N.A.	Frodi
N.A.	Perdite finanziarie
N.A.	Decifratura non autorizzata della pseudonimizzazione
N.A.	Pregiudizio alla reputazione
N.A.	Perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari)
N.A.	Conoscenza da parte di terzi non autorizzati
N.A.	Qualsiasi altro danno economico o sociale, significativo

Gravità dell'Impatto che una distruzione non autorizzata o perdita (**perdita di disponibilità**) dei dati personali - raccolti attraverso i canali di segnalazione interni - potrebbe avere sull'Interessato.
La gravità dell'impatto va considerata separatamente per le categorie di dati personali di cui agli articoli 9 e 10 del RGPD e, precisamente:

TIPOLOGIA DATO	GRAVITA' IMPATTO
DATI COMUNI	**ALTO**
DATI SENSIBILI (ART. 9 RGPD)	**ALTO**
DATI GIUDIZIARI (ART. 10 RGPD)	**ALTO**

Nell'ambito delle operazioni di trattamento derivante dall'utilizzo di canali di segnalazione interni, l'impatto complessivo della perdita di disponibilità è da considerarsi **ALTO**, in considerazione del fatto che il contenuto delle segnalazioni e dei documenti eventualmente prodotti dal segnalante può determinare l'assunzione di provvedimenti (disciplinari e giudiziari) ad elevato impatto sui diritti e le libertà del segnalante e delle persone indicate come possibili responsabili delle condotte illecite o di quelle a vario titolo coinvolte nelle vicende segnalate.

D.1.4. Impatto complessivo

Al termine delle valutazioni condotte, sono ottenuti tre diversi livelli di impatto (per la perdita di riservatezza, integrità e disponibilità).

Il più alto di questi livelli è considerato come il risultato finale della valutazione dell'impatto, relativo al trattamento complessivo dei dati personali.

La valutazione dell'impatto complessivo del trattamento mediante canali di segnalazione interni è:

	BASSO
	MEDIO
X	ALTO
	MOLTO ALTO

D.2. Analisi delle minacce

Una minaccia è qualsiasi circostanza od evento che abbia il potenziale di influire negativamente sulla sicurezza dei dati personali.

In questa fase, l'obiettivo del Titolare del trattamento è comprendere le minacce relative all'ambiente generale del trattamento dei dati personali (esterno o interno) e valutarne la probabilità (probabilità di accadimento della minaccia).

Il rischio di un evento dannoso per i diritti degli interessati deriva dall'esposizione del dato a una o più minacce; quindi, identificare i rischi implica sempre considerare la minaccia che potrebbe originarli e anche le conseguenze che dalla stessa possono determinarsi.

Riprendendo la soprariportata classificazione dele minacce, avuto riguardo al tipo di violazione dei dati personali che possono determinare:

violazione della riservatezza	in caso di divulgazione dei dati personali o accesso agli stessi non autorizzati o accidentali
violazione dell'integrità	in caso di modifica non autorizzata o accidentale dei dati personali
violazione della disponibilità	in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali

Fonti di rischio che possono coinvolgere il trattamento dei dati raccolti attraverso canali di segnalazione interni:

X	Azione intenzionale interna
X	Azione intenzionale esterna
X	Azione accidentale interna
X	Azione accidentale esterna

Tradizionalmente si individuano le seguenti **tipologie di accadimento**, dalle quali si possono originare delle fonti di rischio.
Le fonti di rischio possono essere rappresentate da:
- **persona**, interna o esterna all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, ...);
- **fonte non umana** (acqua, fuoco, eventi naturali, materiali pericolosi, virus informatici, ecc.) che può essere all'origine di un rischio. Può essere un incidente od un sinistro verificatosi presso uno dei soggetti incaricati del trattamento od anche presso Contitolari e Responsabili del trattamento

Possono costituire una "**fonte di rischio umana interna**" le seguenti situazioni:
- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.
Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.
Possono costituire una "**fonte di rischio umana esterna**" le seguenti situazioni:
- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio;
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo;
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine;

- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

E' possibile derivare i seguenti tre **scenari di rischio**:

accesso illegittimo	violazione della riservatezza
modifiche indesiderate	violazione dell'integrità
perdita dei dati	violazione della disponibilità

D.3 Analisi della probabilità di verificazione

Analogamente a quanto fatto in relazione alla valutazione dell'impatto, la **valutazione della probabilità di accadimento** della minaccia può essere solo qualitativa, in quanto strettamente correlata allo specifico ambiente di trattamento dei dati personali.

La probabilità fa riferimento alla possibilità che il rischio si concretizzi.

Nell'ambito dell'approccio suggerito dall'ENISA, vengono definiti tre livelli di probabilità di occorrenza della minaccia, ovvero:

BASSO	è improbabile che la minaccia si materializzi
MEDIO	è possibile che la minaccia si materializzi
ALTO	è probabile che la minaccia si materializzi

L'approccio suggerito dall'ENISA definisce **altresì quattro aree di valutazione** per la probabilità di insorgenza della minaccia e guida il controllore attraverso di esse, vale a dire:
- Risorse di rete e tecniche (hardware e software);
- Processi/procedure relative al trattamento dei dati personali;
- Soggetti coinvolti nel trattamento;
- Settore di attività e scala del trattamento.

D.3.1. Risorse di rete e tecniche (hardware e software)

	SI	NO
Una parte del trattamento dei dati personali viene eseguita tramite Internet?	**X**	
È possibile fornire l'accesso a un sistema interno di trattamento dei dati personali tramite Internet (ad es. per determinati utenti o gruppi di utenti)?	**X**	
Il sistema di trattamento dei dati personali è interconnesso con un altro sistema o servizio IT esterno o interno all'Ente?		**X**
Le persone non autorizzate possono accedere facilmente all'ambiente di elaborazione dei dati?		**X**
Il sistema di trattamento dei dati personali è progettato, implementato o mantenuto senza seguire le best practises in materia?		**X**

Valutazione di **probabilità**:

	BASSO (1)
X	MEDIO (2)
	ALTO (3)

D.3.2. Processi e procedure relativi all'operazione di trattamento dei dati personali

	SI	NO
I ruoli e le responsabilità in relazione al trattamento dei dati personali sono vaghi o non sono chiaramente definiti?		X
L'uso accettabile della rete, del sistema e delle risorse fisiche all'interno dell'organizzazione è ambiguo o non è chiaramente definito?		X
I dipendenti possono portare e utilizzare i propri dispositivi per connettersi al sistema di trattamento dei dati personali?		X
I dipendenti sono autorizzati a trasferire, archiviare o altrimenti elaborare dati personali al di fuori dei locali dell'Ente?		X
Le attività di trattamento dei dati personali possono essere eseguite senza che vengano creati file di registro?		X

DETTAGLI: il RPCT ed i soggetti dal medesimo delegati ad accedere alle segnalazioni pervenute attraverso canali interni, sono sottoposti ad adeguata formazione e puntuali istruzioni.

Valutazione di **probabilità**:

X	BASSO (1)
	MEDIO (2)
	ALTO (3)

D.2.3. Soggetti coinvolti nel trattamento dei dati personali

	SI	NO
Il trattamento dei dati personali è effettuato da un numero indefinito di dipendenti?		**X**
Una parte dell'operazione di elaborazione dei dati è svolta da un contraente/terza parte (responsabile del trattamento)?		**X**
Gli obblighi delle parti/persone coinvolte nel trattamento dei dati personali sono ambigui o non chiaramente indicati?		**X**
Il personale coinvolto nel trattamento dei dati personali non ha familiarità con le questioni di sicurezza?		**X**
I soggetti coinvolti nell'operazione di trattamento dei dati trascurano di archiviare e/o distruggere in modo sicuro i dati personali?		**X**

DETTAGLI: il RPCT ed i soggetti dal medesimo delegati ad accedere alle segnalazioni pervenute attraverso canali interni, sono sottoposti ad adeguata formazione e puntuali istruzioni.

Valutazione di **probabilità**:

X	BASSO (1)
	MEDIO (2)
	ALTO (3)

D.3.4. Settore di operatività e scale di rilevanza del trattamento

	SI	NO
Ritieni che il settore di attività del Titolare sia soggetto ad attacchi informatici?	**X**	
Il Titolare del trattamento ha subito attacchi informatici o altri tipi di violazione della sicurezza negli ultimi due anni?		**X**
Il Titolare ha ricevuto nell'ultimo anno segnalazioni e/o reclami in merito alla sicurezza del sistema informatico (utilizzato per il trattamento dei dati personali)?		**X**
Le operazioni di trattamento riguardano un grande volume di persone e/o dati personali?		**X**
Esistono best practices o disposizioni normative di sicurezza specifiche, per il settore di attività del Titolare del trattamento, che non sono state adeguatamente seguite?		**X**

DETTAGLI: il settore delle pubbliche amministrazioni è recentemente risultato essere vittima di attacchi informatici da parte di malintenzionati. Tuttavia, questo Titolare del trattamento non ha subito violazioni di sicurezza con riferimento al proprio sistema informativo, che risulta adeguatamente protetto attraverso l'adozione delle misure tecniche ed organizzative descritte in precedenza.

Valutazione di **probabilità**:

	BASSO (1)
X	MEDIO (2)
	ALTO (3)

D.3.5. Valutazione della probabilità di occorrenza delle minacce

La **probabilità di occorrenza finale** della minaccia viene calcolata dopo aver sommato i diversi punteggi ottenuti in relazione a ciascuna area.

Il risultato della somma determinerà il livello complessivo di probabilità di verificazione delle minacce sulla scorta della tabella che segue.

Somma globale della probabilità di occorrenza di una minaccia	**Livello di probabilità delle minacce**
4-5	BASSO
6-8	MEDIO
9-12	ALTO

Valore numerico della probabilità complessiva (dato dalla sommatoria dei punteggi attribuiti nei precedenti paragrafi:

PARAGRAFO	**PROBABILITÀ**	**VALORE**
D.2.1	MEDIO	2
D.2.2	BASSO	1
D.2.3	MEDIO	1
D.2.4	MEDIO	2
TOTALE	**MEDIO**	**6**

Livello globale di probabilità delle minacce: MEDIA

D.3. Valutazioni e Piano di trattamento dei rischi

Considerato che:
- a norma dell'**articolo 35, paragrafo 9, del RGPD** "*Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti*";
- a norma dell'**articolo 36, paragrafo 1, del RGPD** "*Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*";

Con particolare riferimento alla c.d. **consultazione preventiva** di cui all'art. 36 del RGPD, si recepiscono le indicazioni contenute nelle Linee Guida rilasciate dal Gruppo di lavoro articolo 29 per la protezione dei dati, come modificate e adottate da ultimo il 4 ottobre 2017 (**WP 248 rev.01**), a tenore delle quali "*Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo*".
"*Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5)*"

Ritenuta la non necessità di procedere ad acquisire il parere degli interessati, trattandosi di trattamenti di dati personali posti in essere dal Titolare, nell'ambito della gestione dei canali di segnalazione interni, sono necessari per dare attuazione agli obblighi di legge ed ai compiti d'interesse pubblico previsti dalla disciplina di settore, la cui osservanza è condizione di liceità del trattamento (artt. 6, par. 1, lett. c) ed e) e parr. 2 e 3, 9, par. 2, lett. b) e g), 10 e 88 del RGPD, nonché 2-ter e 2-sexies del Codice).

Acquisito il parere del Responsabile della Protezione dei Dati Personali (RPD)

Alla luce delle informazioni raccolte e dei risultati della presente valutazione di impatto, **SI RITIENE**:

X	possibile procedere con l'attivazione dei canali di segnalazione interni e l'avvio del trattamento senza ulteriori misure tecniche e organizzative
N.A.	possibile procedere con l'attivazione dei canali di segnalazione interni e l'avvio del trattamento, ma si suggerisce di implementare le misure tecniche e organizzative specificamente indicate
N.A.	possibile procedere con l'attivazione dei canali di segnalazione interni e l'avvio del trattamento, solo dopo aver implementato le misure tecniche e organizzative ulteriori specificamente indicate
N.A.	necessario/opportuno raccogliere le opinioni degli interessati o dei loro rappresentanti, in merito al trattamento
N.A.	necessario consultare l'Autorità di controllo prima di iniziare il trattamento

D.4. Formalizzazione dei risultati, revisione ed aggiornamento

Tutta la documentazione prodotta all'interno del processo di DPIA, partendo dal censimento e descrizione del trattamento, passando dalle valutazioni preliminari per arrivare, quando necessario, al calcolo di analisi dei rischi e relativo piano di trattamento, concorre alla realizzazione del presente report finale, in grado di dimostrare, oltre ovviamente ai risultati ottenuti, la corretta esecuzione formale del processo e la sua aderenza ai requisiti richiesti dalla normativa di protezione dei dati personali.

Il report deve inoltre esplicitare la frequenza di aggiornamento del DPIA, tanto maggiore quanto più si utilizzino tecnologie in evoluzione o si prevedono potenziali variazioni nei processi di trattamento.

La presente DPIA sarà sottoposta a revisione ed aggiornamento, qualora ciò si rendesse necessario a seguito della modifica di taluno dei suoi elementi costitutivi. In ogni caso, sarà oggetto di nuova valutazione con cadenza annuale.

L'attività di revisione ed aggiornamento è condotta dal soggetto designato dal Titolare del trattamento, il quale vi provvede coinvolgendo il Responsabile della Protezione dei Dati Personali (DPO).