Valutazione di Impatto o Data Protection Impact Assessment
Processo di Gestione del Whistleblowing

Allegato alla Delibera Giunta Comunale n. ..... del .....

Comune di Vedano Olona

Sommario

1. Premessa

Il regolamento europeo sul trattamento dei dati impone al titolare di attuare delle azioni per la protezione delle informazioni e per l'applicazione dei diritti degli interessati. Il trattamento dei dati ha maggiori livelli di rischio quando si attua un monitoraggio sistemico dei comportamenti degli interessati, o per il gran numero dei soggetti coinvolti, le tecnologie utilizzate di cui sono magari trattati dati personali particolari, o anche per una combinazione di questi e altri fattori.
Tra le procedure che il Titolare deve attuare rientra quanto previsto all'art. 35 del GDPR, che prevede una valutazione preventiva dell'impatto dei trattamenti previsti sulla protezione dei dati, anche in considerazione di possibili rischi per i diritti e le libertà delle persone fisiche (di seguito, "DPIA").
La Valutazione d'Impatto sulla Protezione dei Dati è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.
La DPIA è un processo dinamico, che ha l'obiettivo di verificare il livello di rischio, e di attuazione dei diritti degli interessati derivanti dal trattamento dei dati e di identificare eventuali azioni per ridurre il rischio stesso.

2. Obiettivo del documento

Il presente documento ha l'obiettivo di descrivere il processo metodologico con cui viene effettuata la DPIA svolta dal Comune di Vedano Olona, i risultati della stessa in relazione ai trattamenti concernenti l'attivazione di un processo per la gestione del whistleblowing.
Attraverso l'analisi verranno identificate le misure tecniche, organizzative e procedurali da adottare per un corretto trattamento dei dati e il contenimento dei livelli di rischi insiti nel processo di trattamento in seguito alle misure di protezione adottate. Nel caso in cui il risultato della valutazione di Impatto presenti un rischio elevato prima di attuare il trattamento deve essere fatta consultazione preventiva con l'autorità garante della protezione dei dati.

3. Normativa di riferimento

- Regolamento UE n. 2016/679 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;
- Art 35 del GDPR: Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi;
- 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 adottate il 4 aprile 2017 (versione successivamente emendata e adottata il 4 ottobre 2017);
- D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni;
- Legge 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
- D.Lgs. n. 165/2001, "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", introduce l'articolo 54-bis, intitolato "Tutela del dipendente pubblico che segnala illeciti";
- Legge 179/2017 sul Whistleblowing approvata il 15/11/2017 a tutela del dipendente pubblico e privato, che prevede che sia predisposto "almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante";
- Regolamento ANAC del 01 luglio 2020 per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54 bis Decreto legislativo n. 165/2001;

- PNA (Piano Nazionale Anticorruzione) 2019 Delibera ANAC n. 1064 del 13 novembre 2019:Il RPCT, oltre a ricevere e prendere in carico le segnalazioni, attua gli atti necessari ad una prima attività di verifica e di analisi delle segnalazioni ricevute da ritenersi obbligatoria in base al co. 6 dell'art. 54-bis;
- Delibera ANAC n. 469 del 9 giugno 2021 L'ANAC, che contiene le "Linee guida in materiadi tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)", con la chiara indicazione che le segnalazioni, al fine di tutelare il segnalante, debbano essere trattate con sistemi informatizzati e crittografici.

4. Definizioni

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

Dato Personale Particolare 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."

Probabilità: valutazione della frequenza di accadimento di un evento, in funzione di eventi esterni non determinabili, delle vulnerabilità in essere e di eventuali contromisure implementate.

Impatto: indicazione del livello di incidenza di un evento che può compromettere la riservatezza, l'integrità e la disponibilità dei dati e dei diritti degli interessati;

Minaccia: evento potenziale, accidentale o deliberato, che, nel caso accadesse, produrrebbe undanno per l'interessato;

Vulnerabilità: debolezza intrinseca del sistema di gestione del dato che, qualora si realizzasse una minaccia, produrrebbe un danno all'interessato;

Rischio: è uno scenario descrittivo di un evento e delle relative conseguenze, che sono stimate intermini di gravità e probabilità» per i diritti e le libertà. Il rischio in questa procedura è sempre riferitoall'interessato

Contromisure: interventi tecnologici, procedure organizzative che possono essere implementate al fine di mitigare il Rischio Privacy associato ad ogni sistema o archivio e quindi diminuire il Rischio;

DPIA: data protection impact assessment

5. Campo di Applicazione

La presente analisi si applica al trattamento dei dati relativi al processo di whistleblowing attivato dal Comune di Vedano Olona.

6. Compiti e responsabilità

Titolare dei trattamenti
La responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare nemonitora lo svolgimento consultandosi con il responsabile della protezione dei dati (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore.

Amministratore di sistema Informativo
Partecipa al processo di valutazione dei rischi e alla attuazione delle contromisure per il contenimento dei rischi.

Responsabile della protezione dei Dati
Il responsabile della protezione dei dati, fornisce un parere in merito alla valutazione di impatto. Valuta inoltre i passi da intraprendere per la comunicazione all'autorità garante della protezione dei dati se il risultato della valutazione di impatto rileva un livello di rischio elevato per i dati degliinteressati.

Componente del Team di Lavoro
La valutazione di impatto può richiedere la partecipazione di esperti dei processi di trattamento e della tecnologia utilizzata. Il soggetto in questione può essere sia un soggetto interno all'organizzazione o un soggetto esterno. Lo stesso è tenuto a fornire un apporto alla conduzionedella DPIA nelle varie fasi.

7. Descrizione del contesto relativo al trattamento dei dati

Il Comune di Vedano Olona in ottemperanza alla Legge 179/2017 sul Whistleblowing ha avviato un'attività di adeguamento del processo di gestione delle segnalazioni che tiene conto anche dei recenti provvedimenti adottati dall'ANAC.
A tal fine l'ente ha valutato di dotarsi di una piattaforma applicativa che consenta di gestire il processo di segnalazione di illeciti e che rispetti le disposizioni dell'Autorità Nazionale per l'Anti Corruzione.
L'analisi effettuata ha considerato la soluzione applicativa sviluppata da whistleblowing solution di cui si allega il documento tecnico rilasciato dal fornitore che ne descrive le caratteristiche tecniche ed infrastrutturali. (Documentazione Tecnica A Supporto Del Titolare Per La Valutazione Di Impatto Sulla Protezione Dei Dati Personali – documento aggiornato il 11 gennaio 2023)

8. Attività di trattamento

DESCRIZIONE DELL'ATTIVITA' DI TRATTAMENTO	
Titolare del trattamento	Comune di Vedano Olona
Contitolare del trattamento	Non presente
Area che gestisce il trattamento	Responsabile dell'anticorruzione del Comune nella persona del segretario comunale
Settore/ufficio	Responsabile dell'anticorruzione del Comune nella persona del segretario comunale
Altri soggetti che accedono alla banca dati	Nessun soggetto accede ai dati della piattaforma che sono salvati in modalità cifrata
Incaricati al trattamento	Non sono previsti soggetti autorizzati al trattamento se non il responsabile dell'anticorruzione
Soggetto terzo qualificato come responsabile del trattamento	Whistleblowing PA che fornisce la piattaforma applicativa in modalità SAAS e gestisce la manutenzione della piattaformaapplicativa
Soggetto terzo qualificato come sub-responsabile del trattamento	Seeweb > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) Transaparency International Italia > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per lacollaborazione nella gestione del sistema di whistleblowing
DPO	Riferimenti del DPO pubblicati sul sito istituzionale del Comune
Descrizione del trattamento	
Finalità del trattamento	Attivazione piattaforma applicativa per la gestione del processo di whistleblowing in modalità digitale incluse le attività di segnalazione di reati o irregolarità di cui siano venuti a conoscenza i dipendenti dell'ente in ragione di un rapporto di lavoro
Base giuridica del trattamento	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. Il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento.
Tipologia di dati trattati	Dati personali dei soggetti che segnalano delle irregolarità Dati relativi alla segnalazione della presunta violazione normativa inmateria di gestione degli appalti
Categorie degli interessati	Dipendenti che segnalano reati o irregolarità
Perimetro in cui i dati sono trattati	I dati vengono trattati nell'ambito del processo di gestione delle segnalazioni di irregolarità nella gestione dei procedimenti di appalto come previsto dalle disposizioni normative e dalle circolarità dell'ANAC.
Modalità di trattamento	I dati vengono trattati in formato digitale, attraverso la piattaforma Applicativa di whistleblowing che gestisce i processi di comunicazione e salvataggio dei dati in modalità cifrata. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono

	configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie alpasso con lo stato dell'arte della ricerca tecnologica in materia.
Tempi di conservazione dei dati	Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.
Destinatari a cui i dati sono comunicati	ANAC Autorità giudiziaria Altri soggetti in nel rispetto della normativa di legge
Diffusione dei dati	I dati non sono soggetti a diffusione
Valutazione della necessità e della proporzionalità del trattamento	
Necessità e proporzionalità del trattamento.	Al fine di rendere efficace e di digitalizzare il processo di whistleblowing il Comune di Vedano Olona intende adottare la piattaforma applicativa sviluppata whistleblowing solution.
È stata effettuata una consultazione preventiva con gli interessati al trattamento	Le caratteristiche del processo di trattamento non prevedono laconsultazione preventiva degli interessati
Asset usati per il trattamento	
Luoghi fisici	La piattaforma applicativa viene erogata in modalità SaaS ed è installata presso provider identificato dal fornitore della soluzione applicativa.
Hardware	L'architettura di sistema è principalmente composta da: • Un cluster di due firewall perimetrali; • Un cluster di due server fisici dedicati; • Una Storage Area Network pienamente ridondata.
Software	La piattaforma informatica di segnalazione è basata sul software GlobaLeaks1. In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile. Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale
Reti di comunicazione	Le reti di trasmissioni dei dati usano protocolli sicuri di cifratura
Possibilità accesso remoto	Non è prevista questa modalità di accesso da parte di soggetti terzi. L'applicativo è una piattaforma web accessibile attraverso browserin modalità SAAS.
Diritti degli interessati	

Come sono stati informati gli interessati	Il titolare ha predisposto una informativa nella quale sono indicate le policy relative al trattamento dei dati.
Accesso ai dati	L'accesso ai dati è consentito solo al soggetto interessato che effettua la segnalazione e al responsabile dell'anticorruzione
Rettifica dei dati	La rettifica dei dati è consentita solo al soggetto interessato che effettua la segnalazione
Cancellazione	I dati vengono cancellati al termine dell'iter di gestione del procedimento nel rispetto della normativa di legge.
Portabilità	Diritto non previsto per il tipo di trattamento
Opposizione	L'inserimento dei dati per segnalazione di un illecito è su base volontaria per cui questo principio non si applica
Limitazione di trattamento	I dati vengono trattati per un tempo limitato come indicato nell'informativa
Revoca del consenso	Il trattamento non si basa sul consenso al trattamento dei dati
Limitazione della finalità	I dati sono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità. L'accesso ai dati è regolamentato e consentito solo al responsabile dell'anticorruzione Le finalità sono rese note all'interno nell'informativa relative al trattamento dei dati
Limitazione della conservazione	I dati sono conservati in modalità cifrata che non consentel'identificazione degli interessati se non ai soggetti autorizzati al trattamento. Il tempo di conservazione rispetta le disposizioni normative e procedurali definite da ANAC
Integrità e riservatezza	La piattaforma applicativa adotta misure di sicurezza tecnologicheper la protezione dei dati quali • Registrazione delle operazioni eseguite in file di log che non prevedono l'identificazione dei soggetti che hanno fatto la segnalazione; • Protezione degli apparati di elaborazione; • Cifratura dei dati registrati; • Utilizzo prettamente di piattaforme open source
Coinvolgimento del DPO	Il DPO nominato dall'Ente è stato consultato nella predisposizione della DPIA

9. Valutazione Dei Rischi Per Diritti E Libertà E Per La Protezione Dei DatiDegli Interessati

La valutazione del rischio è il processo complessivo di: identificazione del rischio, analisi del rischio eaccertamento (in senso stretto) del rischio. I rischi possono essere valutati a livello di organizzazione,di dipartimento, per singoli trattamenti, per processi o attività individuali o per rischi specifici.
La valutazione del rischio fornisce una comprensione delle loro cause, delle conseguenze e connesse probabilità. Ciò costituisce l'input a decisioni del tipo:

- se l'attività di trattamento deve essere intrapresa, o no
- se i rischi devono essere trattati - scegliere tra opzioni con rischi differenti
- mettere in priorità le opzioni di trattamento dei rischi (riduzione, trasferimento, accettazione e monitoraggio).
- selezionare le strategie più appropriate per il trattamento degli stessi, che possono condurre ad un livello tollerabile.

Per fornire una misurazione sul livello di rischio a cui l'organizzazione va incontro si utilizza un metodo quantitativo per valutare l'indice di rischio attraverso una valutazione legata a diversi parametri

Le definizioni applicate ai fini dell'analisi dei rischi sono:

Probabilità: frequenza del verificarsi delle conseguenze;
Impatto: qualunque conseguenza negativa derivante dal verificarsi dell'evento;
Indice Rischio (ID): combinazione della probabilità di accadimento di un danno e della gravità di quel danno.
Per misurare il rischio l'ente utilizza la relazione:

R: P x D e le seguenti scale:

Criteri per determinale la probabilità di accadimento		
P	Livello di probabilità	Criteri di valutazione
4	Alta	Accade di frequente
3	Media	Può accadere diverse volte
2	Bassa	Può accadere talvolta
1	trascurabile	Improbabile

Criteri per determinale l'Impatto		
P	Livello di probabilità	Criteri di valutazione
4	Alta	Grave danno per i diritti e le libertà degli interessati
3	Media	danno Medio per i diritti e le libertà degli interessati
2	Bassa	danno Basso per i diritti e le libertà degli interessati
1	trascurabile	danno Trascurabile

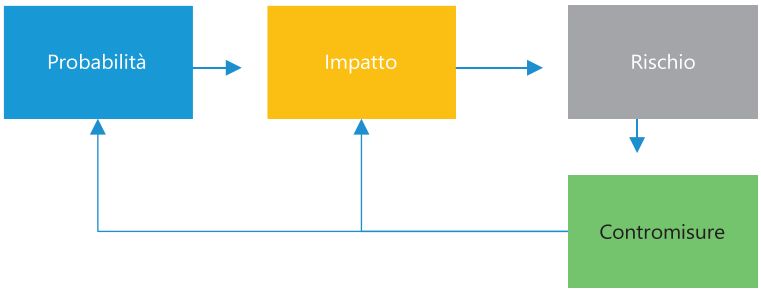
Il comune ha sviluppato questa attività ed ha sintetizzato il risultato di questo lavoro nella matrice diseguito allegata.

Probabilità					
	IR	1	2	3	4
danno	1	1	2	3	4
	2	2	4	6	8
	3	3	6	9	12
	4	4	8	12	16

	Rischio basso		Rischio medio		Rischio alto		Rischio altissimo
	Monitorare		Monitorare		Azione Correttiva o piano di Miglioramento		Azione Correttiva

Nel caso in cui il rischio relativo ad un'attività di trattamento sia alto o altissimo si deve procedere con una mitigazione dello stesso adottando un'azione per il contenimento e valutare in seguito l'esito di questa azione in termini di indice di rischio.

Metodo valutazione del Rischio



10. Valutazione di impatto

Nella tabella di seguito riportata sono riportati gli esiti della valutazione di impatto

10.1 Misure di Sicurezza attivate

Di seguito vengono descritte le misure di sicurezza adottate dall'ente per la protezione dei dati Trattandosi di un servizio applicativo parte delle misure di sicurezza vengono gestite dal fornitoredell'applicazione, ma parte del trattamento dei dati viene eseguito nel perimetro della sede dell'ente e del sistema informativo comunale, motivo per cui nell'analisi dei rischi si fa riferimentoanche a questi aspetti.

Misure sicurezza edificio
nessuna
Misure sicurezza Data Center ed infrastruttura di rete
Un cluster di due firewall perimetrali;
Un server fisico dedicati;
Una storage area network pienamente ridondata.
Misure sicurezza adottate dalla Piattaforma Applicativa
Dati salvati in modalità cifrata
Registrazione dei log anonimizzata
L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLANal fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definite insieme di amministratori di sistema;
Tutti i dispositivi utilizzati quali applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali indirizzi IP e User Agents
L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologicain materia.
Misure sicurezza sala server dell'ente
Accesso al solo personale autorizzato tramite porta blindata chiusa a chiave
Estintori installati localmente
Climatizzazione della sala server
Misure sicurezza organizzative
Nomina del responsabile dell'anticorruzione
Approvazione di una linea guida relativa alla protezione dei dati
Misure sicurezza tecnologica dell'ente
Server alimentati con batterie di continuità
Impianto elettrico a norma
Cartelle in cui vengono eventualmente conservate le registrazioni profilate, ed autorizzazioni di accesso ai soli incaricati
Protezione del server tramite tools di sicurezza ed antivirus
Protezione delle postazioni di lavoro tramite tools di sicurezza ed antivirus
Protezione della rete tramite apparati perimetrali (firewall)
Vengono fatte delle copie di sicurezza delle cartelle del server nel quale sono eventualmente conservate i dati e l'istruttoria relativa alle segnalazioni relative al processo di whistleblowing

Di seguito viene riportato lo schema con cui viene effettuata l'analisi dei rischi in materia ditrattamento dei dati avente come elemento di protezione i dati ed i diritti dell'interessato.

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Non rispetto diritti degli interessati							
Furto di dati	Violazione delle libertà o della dignità per l'interessato	1	3	3	Accesso ai dati è consentito sono a personale autorizzato a cui è associato un profilo di accesso ai dati in funzione della mansione attribuita Il comune ha attuato delle misure di sicurezza tecnologiche per la protezionedei dati Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Rischio che gli interessati possano essere non adeguatamente informati sul trattamento dei loro dati	Reclami degli interessati Violazione delle libertà	2	1	2	L'ente ha predisposto una informativa sul trattamento dei dati che è stata pubblicata sul sito istituzionale del comune		
Rischi che i dati possano essere utilizzati non rispettando i limiti delle finalità per cui sonoraccolti o che vengano raccolti dati eccedenti le finalità previste dal progetto.	Reclami degli interessati	1	2	2	I dati vengono raccolti per finalità legittime in base alle norme di legge in materia di whistleblowing. Il tempo di conservazioni rispetta le finalità del trattamento inerenti la gestione della segnalazione e la necessità di gestire l'istruttoria I dati vengono forniti volontariamente dall'interessato		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
					L'ente ha predisposto una informativa sul trattamento dei dati che è stata pubblicata sul sito istituzionale del comune		
Rischi di accesso nonautorizzato ai dati	Perdita di dignità, violazione delle libertà per l'interessato	2	2	4	L'accesso alle banche dati viene fatto solo da soggetti autorizzati tramite utente protetto da password Il comune ha attuato delle misure di sicurezza tecnologiche per la protezionedei dati Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Rischi che i dati siano conservatiper un periodo non necessariorispetto al trattamento.	Non rispetto nel principio di minimizzazione dei dati Riservatezza Integrità	1	2	2	Il tempo di conservazioni rispetta le finalità del trattamento inerenti la gestione della segnalazione e la necessità di gestire l'istruttoria		
Rischi che l'interessato possa avere difficoltà ad esercitare i suoi diritti (es. diritto allacancellazione o modifica del dato) o che i suoi diritti venganoviolati	Reclami degli interessati Sanzioni dell'autorità garante	1	2	2	I dati sono accessibili agli interessati attraverso procedure di accesso allapiattaforma Le policy di trattamento die dati sono descritte nell'informativa relativa altrattamento dei dati Il comune ha attuato delle misure di sicurezza tecnologiche per la protezionedei dati		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
					Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Trattamento dei dati non conforme alla normativa di legge o alle linee guida dell'Autorità garante per la protezione dei dati.	Reclami degli interessati Sanzioni dell'autorità garante	2	2	4	I dati vengono raccolti per finalità legittime in base alle norme di legge in materia di whistleblowing.		
					Verifica della corretta gestione delleprocedure di trattamento dei dati e delle tecnologie utilizzate.		
Rischi fisici sede dell'ente							
Incendio	disponibilità Integrità	1	2	2	Impianti elettrici manutenuti in base alle norme di legge I locali dell'ente sono dotati di estintori		
Allagamento	disponibilità Integrità	1	2	2	L'edificio dell'ente è distante da corsi d'acqua e bacini idrici. Storicità dell'evento bassa		
Distruzione di strumentazione da parte di personemalintenzionate	disponibilità Integrità	1	2	2	Le misure di sicurezza dell'edificio sono adeguate, Storicamente non si sono mai verificati eventi di questo tipo. Una porzione del perimetro della sededell'ente è sottoposta a video sorveglianza Accesso ai locali in cui sono installati gli apparati del sistema informativo tramite porta chiudibile a chiave		
Attacchi Fisici, Furti, Attivandalici	disponibilità Integrità	1	2	2	Le misure di sicurezza dell'edificio sono adeguate.		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
					Una porzione del perimetro della sededell'ente è sottoposta a video sorveglianza Accesso ai locali in cui sono installati gli apparati della video sorveglianza tramite armadio chiudibile a chiave		
Fenomeni climatici - eventi calamitosi (Uragani, Nevicate)	disponibilità Integrità	1	2	2	Storicamente non si sono verificati eventi climatici dannosi		
Terremoti	disponibilità Integrità	1	2	2	Storicamente non si sono verificati eventi naturali dannosi quali terremoti. Rischio sismico basso		
Furto degli apparati	Disponibilità Riservatezza Integrità	2	2	4	I dispositivi sono installati in luoghi protettie/o difficilmente accessibili.		
Accesso non autorizzati a localie/o in aree ad accesso ristretto	Riservatezza Integrità	2	1	2	I dispositivi di memorizzazione dei dati sono installati in locali ad accesso protetto.		
Sicurezza delle Rete Trasmissione Dati e della Rete Informatica dell'ente							
Rischi legati ad attacchi informatici	Disponibilità Riservatezza Integrità	2	2	4	L'ente ha adottato misure di sicurezza adeguate alla protezione dei dati(apparato di sicurezza perimetrale, software di protezione sugli apparati server e sulle postazioni di lavoro)		
Rischi legati all'accesso daparte di soggetti non autorizzati al trattamento dei dati	Disponibilità Riservatezza Integrità	1	2	2	L'accesso ai dati avviene tramite regole di autenticazione e profili diversi di accesso aidati		
					Le società esterne che eseguono interventi di manutenzione ed assistenza sulla piattaforma applicativa sono state qualificate e nominate responsabili del		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
					trattamento dei dati ed il loro operato verificato dal personale della Polizia Locale		
Accesso non autorizzato ai locali per omessa sicurezza dellastruttura	Disponibilità Riservatezza Integrità	1	2	2	I locali nei quali sono installati gli apparati informatici sono adeguatamente protetti (edificio parzialmente video sorvegliato, porta blindata di accesso sala server con serratura)		
Mancanza di energia elettrica o instabilità della stessa	Disponibilità	1	1	1	Evento raro con conseguenze accettabili Server alimentato con batterie di continuità		
Malfunzionamento per mancanza interventi di manutenzione che determinano anche delle vulnerabilità informatiche	Disponibilità Riservatezza Integrità	2	2	4	L'ente può contare su società specializzate nella manutenzione della piattaformaapplicativa		
Intercettazione delle informazioni trasmesse sulla rete informatica	Riservatezza	1	2	2	La piattaforma applicativa utilizza protocolli sicuri di trasmissione dei dati		
Sicurezza della infrastruttura su cui è installata la piattaforma di whistleblowing							
Rischi legati ad attacchi informatici	Disponibilità Riservatezza Integrità	2	2	4	Il fornitore della piattaforma applicativa ha attuato delle misure di sicurezza tecnologiche per la protezione dei dati come descritto nella documentazione tecnica fornita		
Rischi legati all'accesso daparte di soggetti non autorizzati al trattamento dei dati	Disponibilità Riservatezza Integrità	1	2	2	L'accesso ai dati avviene tramite regole di autenticazione e profili diversi di accesso aidati		
					La società che gestisce la manutenzione e l'assistenza della piattaforma applicativa èstata nominata responsabile del trattamento dei dati		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Accesso non autorizzato ai locali per omessa sicurezza dellastruttura	Disponibilità Riservatezza Integrità	1	2	2	La piattaforma di whistleblowing è installata in un data center qualificato edotato di idonee misure di sicurezza fisica		
Mancanza di energia elettrica o instabilità della stessa	Disponibilità	1	1	1	La piattaforma di whistleblowing è installata in un data center qualificato e dotato di idonee misure di sicurezza tecnologica		
Malfunzionamento per mancanza interventi di manutenzione che determinano anche delle vulnerabilità informatiche	Disponibilità Riservatezza Integrità	2	2	4	L'ente può contare su società specializzata nella manutenzione della piattaforma applicativa		
Intercettazione delle informazioni trasmesse sulla rete informatica	Riservatezza	1	2	2	La piattaforma applicativa utilizzaprotocolli sicuri di trasmissione dei dati. La soluzione applicativa è installata su datacenter certificato AGID		
Rischi legati ai dati trattati dalla piattaforma di whistleblowing							
Modifica non autorizzata di dati	Riservatezza Integrità	1	2	2	I dati sono adeguatamente protetti per il livello di rischio legato alla modifica od alterazione degli stessi. I dati sono salvato in modalità cifrata		
Comunicazione illecita o non corretta dei dati	Riservatezza	1	2	2	I dati trattati nel processo di whistleblowing non sono soggetti a comunicazione		
Mancata eliminazione dei datial termine del trattamento	Riservatezza	2	2	4	I dati sono salvati in modalità cifrata. I dati al termine dell'istruttoria possono essere cancellati dal segnalatore		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Trasferimento di dati all'estero	Riservatezza Mancato rispetto delle normative di legge	1	2	2	I dati relativi alla gestione del processo di whistleblowing non vengono trasferiti al difuori dello spazio UE		
Danneggiamento delle banche	Disponibilità dei dati	1	2	2	Aggiornamento periodico dellapiattaforma applicativa. Gestione delle copie dei server virtuali su cui è installata la piattaforma di whistleblowing		
Rischi legati all'applicazioni software e agli apparati HW							
sottrazione/alterazione credenziali di autenticazione	Riservatezza Integrità	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate		
Policy di backup non adeguate problemi nelle procedure di gestione delle copie di sicurezza	Disponibilità	1	2	2	La piattaforma è installata su una struttura di server configurata in alta affidabilità. I server virtuali su cui è installata la piattaforma sono periodicamente copiati.		
Uso non autorizzato del software	Riservatezza	1	2	2	Le credenziali di accesso ai dati vengono periodicamente cambiate da parte del responsabile dell'anticorruzione da parte del responsabile dell'anticorruzione		
					I dati sono adeguatamente protetti per il livello di rischio legato al furto o all'accesso non autorizzato		
Malfunzionamento degli apparati o del sw di gestione deidati	Riservatezza Integrità	2	2	4	Rischio di malfunzionamento degli apparati accettabile		
Mancato aggiornamento del software o errori di funzionamento	Riservatezza Integrità	1	2	2	Il software di gestione viene periodicamente aggiornato. Attivato contratto di manutenzione della piattaforma applicativa di whistleblowing		

Descrizione del rischio	Impatto	Prob.	Imp.	Rischio	Misure di contenimento del rischio adottate	Piani di Miglioramento	Rischio residuo
Rischi legati agli utenti							
Errori nel corretto trattamento dei dati da parte del titolare o da personale autorizzato	Disponibilità Riservatezza Integrità	1	2	2	Sensibilizzazione e formazione dei soggetti coinvolti nel trattamento; Istruzioni tecniche o formazione fornita al personale autorizzato al trattamento		
Non consapevolezza nelle procedure di gestione	Disponibilità Riservatezza Integrità	1	2	2	Il personale coinvolto nel trattamento èstato adeguatamente istruito; Il Comune si è avvalso di aziende o professionisti qualificati per l'attivazione della piattaforma di whistleblowing		
Non applicazione delle procedure di trattamento dei dati	Riservatezza Integrità	1	2	2	Sensibilizzazione e formazione dei soggetti coinvolti nel trattamento;Istruzioni tecniche o formazione fornita al personale autorizzato al trattamento		
Trattamento non corretto od illecito	Riservatezza Integrità	1	2	2	L'ente ha avviato procedure conformi alla normativa per una corretta gestione dei dati; I dati sono adeguatamente protetti sia con misure di carattere tecnologico che di protezione fisica		
Diffusione illecita delle immagini	Riservatezza	1	2	2	I dati relativi alla segnalazione di whistleblowing non sono soggetti a diffusione		
comportamenti sleali, dolosi, fraudolenti degli operatori - cancellazione non autorizzata/manomissione di dati	Disponibilità Riservatezza Integrità	1	3	3	I dati salvati dalla piattaforma di whistleblowing sono salvati in modalità cifrata		

11. Conclusione Finale

In seguito all'analisi effettuata, il trattamento non presenta particolari criticità in materia id protezione dei dati e rispetto dei diritti degli intenteresti per cui il Comune di Vedano Olona non deve attuare azioni particolari nel processo di trattamento.

12. Allegati

Scheda tecnica fornita dal fornitore