PROVINCIA
DI PARMA

Valutazione di impatto sul trattamento dei dati personali relativi al sistema di gestione delle segnalazioni di Whistleblowing

Provincia di Parma

Sommario

1. Introduzione

1.1. Oggetto e scopo

Il presente documento svolge la valutazione di impatto sulla protezione dei dati personali ai sensi degli articoli 35 e 36 del Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016 ("GDPR") per i sistemi di gestione delle segnalazioni di Whistleblowing della Provincia di Parma.

1.2. Versione

Le misure tecniche ed organizzative per la protezione dei dati personali evolvono nel tempo in funzione dei miglioramenti tecnologici offerti dal mercato, delle nuove funzionalità richieste dalla gestione delle segnalazioni di Whistleblowing, dei cambiamenti normativi che regolano la particolare tipologia del trattamento (compresi gli interventi del Garante per la protezione dei dati personali e le Linee Guida europee) e delle nuove minacce portate ai sistemi dal mutato assetto politico − economico generale.

Il presente documento svolge la valutazione di impatto tenendo conto dello stato dell'arte al mese di dicembre 2023. Per maggiore chiarezza, si evidenziano nel testo le misure già progettate ma non ancora concluse a tale data e che troveranno piena attuazione nei mesi successivi.

1.3. La valutazione di impatto sulla protezione dei dati (DPIA)

Il GDPR impone una radicale rilettura dei comportamenti in materia di privacy, chiedendo al Titolare del trattamento un approccio non meramente formale alla materia, ma l'adesione al principio di *accountability,* ossia la responsabilizzazione delle figure coinvolte nella gestione della privacy: il Titolare − tenuto conto della natura, del campo di applicazione, del contesto e delle finalità, nonché dei rischi per i diritti e le libertà delle persone fisiche − deve mettere in atto misure tecniche ed organizzative adeguate e costantemente aggiornate per garantire ed essere in grado di dimostrare che il trattamento sia effettuato conformemente al Regolamento stesso.

Un elemento di novità introdotto dal GDPR e che risponde al principio di accountability è rappresentato dall'obbligo di eseguire la c.d. "*Data Protection Impact Assessment*" ("DPIA"), consistente in una valutazione preliminare di impatto posta a garanzia dei diritti del singolo, da svolgere "*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*" (art.35 GDPR).

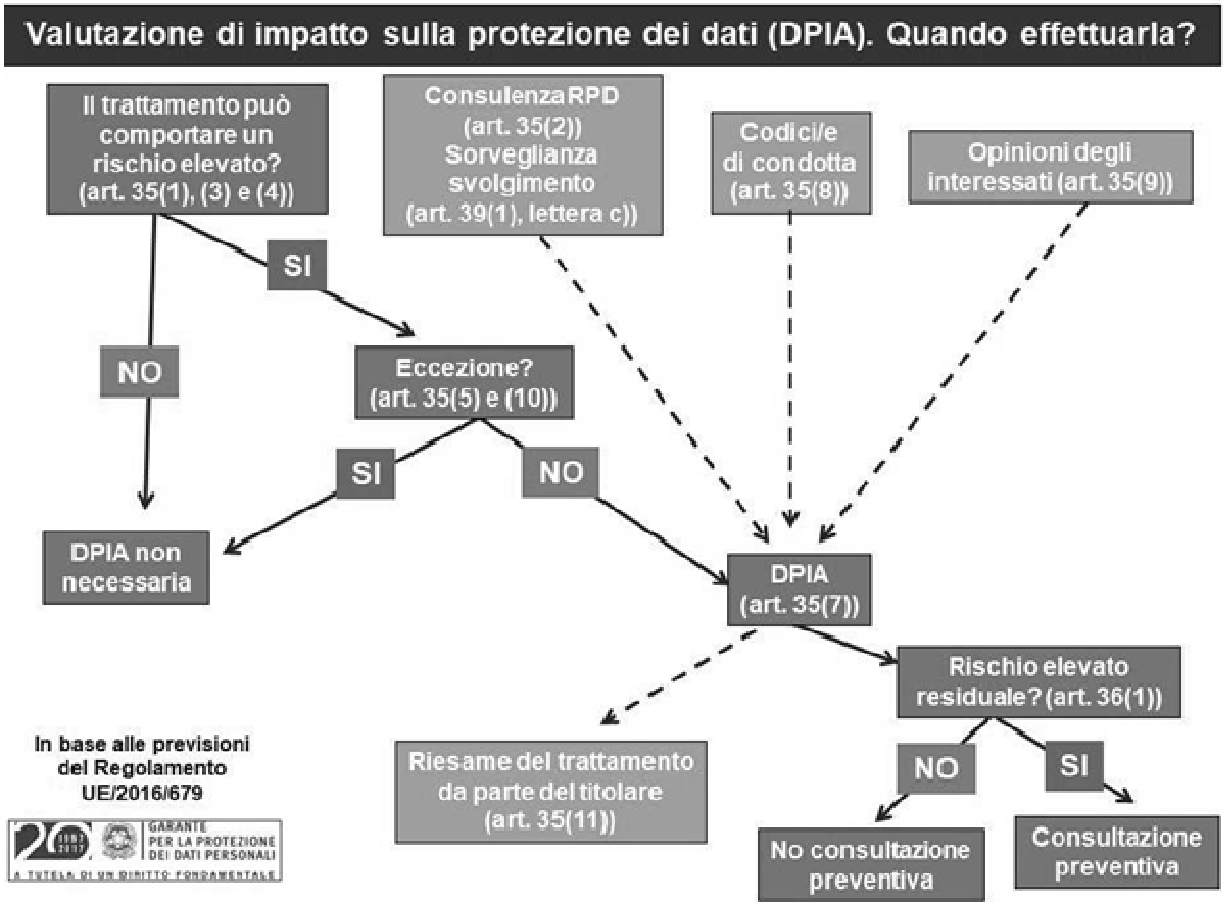
1.4. Le Linee Guida in materia di DPIA (LG−DPIA)

Le "*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*"[1] – WP 248 rev.01 del 13/10/2017 ("LG−DPIA") del Gruppo di Lavoro Articolo 29 per la protezione dei dati[2] forniscono indicazioni operative in materia di DPIA. In particolare, le LG−DPIA specificano il seguente **processo di valutazione**[3] che, partendo da una valutazione iniziale del rischio del trattamento, conduce o meno alla necessità di procedere alla DPIA (art.35 GDPR) e, nel caso in cui il trattamento riesaminato presenti ancora un rischio residuo elevato, alla consultazione preventiva presso il Garante (art.36 GDPR):

1 https://ec.europa.eu/newsroom/article29/items/611236

2 Il Gruppo di lavoro è stato istituito in virtù dell'articolo 29 della direttiva 95/46/CE. È l'organo consultivo indipendente dell'UE per la protezione dei dati personali e della vita privata. I suoi compiti sono fissati all'articolo 30 della direttiva 95/46/CE e all'articolo 15 della direttiva 2002/58/CE.

3 Lo schema del processo di valutazione qui riportato è la versione pubblicata nella sezione dedicata alla DPIA sul sito GPDP: https://www.garanteprivacy.it/valutazione−d−impatto−della−protezione−dei−dati−dpia−



Per quanto riguarda la metodologia di valutazione, ricordato che il GDPR "offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti", l'Allegato 2 delle LG−DPIA individua i seguenti **criteri comuni** che, dettagliando i contenuti obbligatori indicati dall'art.35.7 GDPR, possono dimostrare che una particolare metodologia di valutazione soddisfa la norma:

una descrizione sistematica del trattamento è così fornita (articolo 35, paragrafo 7, lettera a)):

- *la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);*
- *vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;*
- *viene fornita una descrizione funzionale del trattamento;*
- *sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);*
- *si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);*

la necessità e la proporzionalità sono valutate (articolo 35, paragrafo 7, lettera b)):

- *sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):*
- *misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:*
- *finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));*
- *liceità del trattamento (articolo 6);*

- *dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));*
- *limitazione della conservazione (articolo 5, paragrafo 1, lettera e));*
- *misure che contribuiscono ai diritti degli interessati:*
- *informazioni fornite all'interessato (articoli 12, 13 e 14);*
- *diritto di accesso e portabilità dei dati (articoli 15 e 20);*
- *diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);*
- *diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);*
- *rapporti con i responsabili del trattamento (articolo 28);*
- *garanzie riguardanti trattamenti internazionali (capo V);*
- *consultazione preventiva (articolo 36).*

rischi per i diritti e le libertà degli interessati sono gestiti (articolo 35, paragrafo 7 lettera c)):

- *l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:*
- *si considerano le fonti di rischio (considerando 90);*
- *sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;*
- *sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;*
- *sono stimate la probabilità e la gravità (considerando 90);*
- *sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);*

le parti interessate sono coinvolte:

- si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
- si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Le LG−DPIA concludono che "*spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2*".

1.5. Obbligatorietà della DPIA per i sistemi di gestione di segnalazioni di Whistleblowing

L'art. 35 GDPR, al comma 3 riporta un primo elenco di trattamenti per cui è obbligatoria alla DPIA e, al comma 4, chiede alle Autorità nazionali di controllo di redigere e rendere pubblico un elenco di tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati.

Le LG−DPIA enucleano nove criteri tra i quali quelli evocati dal GPDP; nell'ambito di interesse si ricorda:

- **dati relativi a interessati vulnerabili (considerando 75**): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili

possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), **i dipendenti**, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

- **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita " in conformità con il grado di conoscenze tecnologiche raggiunto" (considerando 91), può comportare la necessità di realizzare una valutazione d' impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d' impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi di una valutazione d'impatto sulla protezione dei dati".

A sgomberare il campo da qualsiasi discrezionalità, è intervenuto proprio il Decreto Whistleblowing, D.Lgs n. 24 del 10 marzo 2023, attuativo della direttiva (UE) 2019/1937, che ha disposto l'obbligo di esecuzione di una valutazione di impatto a carico dei titolari del trattamento che devono adottare un sistema di gestione delle segnalazioni.

Nello specifico, il comma 6 dell'art. 13 del Decreto Whistleblowing (che regola gli aspetti connessi alla protezione dei dati personali legati ai Sistemi di Gestione delle Segnalazioni - SGS), stabilisce infatti che i soggetti tenuti ad adottare un SGS "[…] *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*".

Inoltre, lo stesso Garante per la Protezione dei dati personali, nel suo *Parere su uno schema del Decreto Whistleblowing* – aveva sottolineato che: "*L'articolo 13 disciplina il trattamento dei dati personali, sancendo una clausola di generale conformità al Regolamento, al Codice e al d.lgs. 51 del 2018, indicando i ruoli dei soggetti coinvolti nel trattamento,* ***imponendo l'obbligo di procedere alla valutazione d'impatto sulla protezione dei dati*** *e di astenersi dal raccogliere (con immediata cancellazione in caso di raccolta accidentale di dati) i dati personali manifestamente non utili alla gestione di una specifica segnalazione*".

1.6. Conformità della DPIA al GDPR

La DPIA svolta nel presente documento è strutturata in capitoli che rispondono positivamente ai contenuti richiesti dall'art.35.7 GDPR ed alle raccomandazioni contenuti nelle LG−DPIA, nonché alla valutazione finale richiesta dall'art.36.1 GDPR:

GDPR	**Testo dell'articolo**	**Sviluppato nel**
Art. 35.7.a	*una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento*	Capitolo 2 Descrizione del trattamento
Art 35.7.b	*una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità*	Capitolo 3 Necessità e proporzionalità del trattamento

GDPR	Testo dell'articolo	Sviluppato nel
Art. 35.7.c	*una valutazione dei rischi per i diritti e le libertà degli interessati*	Capitolo 4 Gestione del Rischio, rischi per gli interessati, misure di contenimento
art. 35.7.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*	
Art 36.1	*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*	Capitolo 5 Conclusioni

1.7. Abbreviazioni

CPDP	D.Lgs. 196/2003 Codice in materia di protezione dei dati personali
DPIA	Data Protection Impact Analysis: Valutazione di impatto sulla protezione dei dati (art.35 GDPR)
GDPR	General Data Protection Regulation: Regolamento Generale sulla Protezione dei Dati (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016
GPDP	Garante per la Protezione dei Dati Personali ("Garante Privacy" italiano)
SGS	Sistema di Gestione delle Segnalazioni
LG−DPIA	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 − WP 248 rev.01 del Gruppo di Lavoro Articolo 29 per la protezione dei dati

2. Descrizione del trattamento

Il presente capitolo descrive il trattamento svolto fornendo i necessari elementi conoscitivi relativi alla finalità ed ai mezzi del trattamento.

2.1 Contesto e finalità

Il contesto e la finalità del trattamento dei dati personali sono definiti dalla Procedura per la Segnalazione di illeciti o irregolarità", aggiornata e approvata con determina n. 1006 del 14/07/2023 del Responsabile della Prevenzione della Corruzione e della Trasparenza della Provincia di Parma e alla sezione 2.3.6.C "Prevenzione della Corruzione" del PIAO.

Rinviando alla lettura della sopracitata Procedura per i dettagli, si riportano qui sinteticamente gli elementi utili per la valutazione di impatto.

Contesto di applicazione

La procedura disciplina le modalità di segnalazione degli illeciti nell'ambito delle attività di prevenzione della corruzione previste nella sez. 2.3 "Rischi corruttivi e trasparenza" del Piano Integrato Attività e Organizzazione (PIAO) in coerenza con il D. Lgs. n. 24/2023, attuativo della Direttiva Europea n. 1937/2019, che ha raccolto in un unico contesto normativo l'intera disciplina dei canali di segnalazione e delle tutele

riconosciute ai segnalanti, sia nel settore pubblico che privato e dettando una disciplina organica e uniforme, finalizzata ad una maggiore tutela del whistleblower, in modo che quest'ultimo sia maggiormente incentivato all'effettuazione di segnalazione di illeciti.

Finalità

L'obiettivo è quello di fornire indicazioni operative riguardo alla trasmissione e gestione delle segnalazioni e sulle forme di tutela previste nel nostro ordinamento.

Base giuridica

I dati sono acquisiti tramite il SGS per l'adempimento di un obbligo di legge gravante sul titolare del trattamento e connessi all'esercizio di un compito di interesse pubblico.

Procedura per la segnalazione mediante canale interno

Il segnalante può inviare la segnalazione attraverso la procedura informatica "Piattaforma Whistleblowing PA" al sito web pubblicato sul sito istituzionale dell'Ente alla sezione "Amministrazione Trasparente", sottosezione "Altri contenuti – Prevenzione della corruzione".

La procedura per la segnalazione avviene secondo le seguenti modalità:

- viene fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima, nel qual caso sarà presa in carico solo se adeguatamente circostanziata;

- viene ricevuta dal RPCT e da lui gestita mantenendo il dovere di confidenzialità nei confronti del segnalante;

- all'invio della segnalazione, il segnalante riceve un codice numerico di 16 cifre che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta del RPC e dialogare rispondendo a richieste di chiarimenti o approfondimenti;

- la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno dell'Ente che dall'esterno con tutela dell'anonimato garantito in ogni circostanza;

- la piattaforma consente il dialogo, anche in forma anonima, tra il segnalante e il RPC per richieste di chiarimenti o approfondimenti, quindi senza ulteriori contatti.

Le segnalazioni inoltrate potranno essere gestite esclusivamente dal RPCT che accederà alla piattaforma con credenziali riservate e personali nel rispetto delle misure di sicurezza in materia di tutela dei dati personali.

La conservazione dei dati avverà a norma di legge e per il tempo necessario e, qualora i dati fossero costituiti da documenti cartacei, saranno custoditi in armadio chiuso a chiave presso l'ufficio del RPC e accessibile solo allo stesso.

Esaurito il tempo necessario per l'accertamento della fondatezza della segnalazione, per l'adozione di eventuali provvedimenti disciplinari e per la conclusione di eventuali contenziosi avviati, i dati saranno distrutti o resi in forma anonima se necessari per fini statistici.

Canale esterno di segnalazione

L'Autorità Nazionale Anticorruzione (ANAC) ha attivato un canale di segnalazione esterna che il segnalante può utilizzare laddove ricorra una delle seguenti condizioni:

il canale di segnalazione interna non è attivo o, anche se attivato, non è conforme a quanto previsto dall'art. 4 del D. Lgs. n. 24/2023;

la persona segnalante ha già effettuato una segnalazione interna e la stessa non ha avuto seguito;

la persona segnalante ha fondati motivi di ritenere che, se effettuasse una segnalazione interna, alla stessa non sarebbe dato efficace seguito ovvero che la stessa segnalazione possa determinare il rischio di ritorsione;

la persona segnalante ha fondato motivo di ritenere che la violazione possa costituire un pericolo

imminente o palese per il pubblico interesse.

ANAC fornisce sul proprio sito istituzionale le modalità da seguire per l'utilizzo di detto canale.

2.2 Categorie di interessati e di dati personali

Le **categorie di interessati** di cui vengono trattati i dati personali sono i segnalanti e/o i segnalati, nella veste di:

- dipendenti della Provincia di Parma, anche in servizio presso altre Pubbliche Amministrazioni in posizione di comando o distacco;

- dipendenti della Provincia di Parma in periodo di prova;

- soggetti per le quali il rapporto giuridico con la Provincia di Parma non è ancora iniziato, limitatamente alle violazioni riscontrate durante il processo di selezione o in altre fasi precontrattuali;

- pensionati, limitatamente alle violazioni riscontrate prima dello scioglimento del rapporto di lavoro;

- collaboratori, liberi professionisti, consulenti che prestano la propria attività presso la Provincia di Parma;

- dipendenti delle società in house, degli organismi di diritto pubblico o dei concessionari di pubblico servizio, nonché i dipendenti di enti di diritto privato sottoposto a controllo pubblico da parte della Provincia di Parma;

- soggetti con funzioni di amministrazione, direzione, controllo, vigilanza, rappresentanza presso la Provincia di Parma;

- consulenti, collaboratori e fornitori di beni e servizi di cui siano venuti a conoscenza in ragione del proprio rapporto lavorativo con la Provincia di Parma.

Le **categorie di dati personali** trattati:

l'acquisizione e gestione delle segnalazioni dà luogo a trattamenti di dati personali, anche appartenenti a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti a interessati (persone fisiche identificate o identificabili) e, in particolare, i segnalanti o le persone indicate come possibili responsabili delle condotte illecite o quelle a vario titolo coinvolte nelle vicende segnalate.

2.3 Ciclo di vita dei dati personali trattati

Il ciclo di vita dei dati personali trattati è così descrivibile: acquisizione, gestione (istruttoria della segnalazione, in entrata e in uscita), conservazione e cancellazione.

In riferimento al periodo di conservazione della documentazione inerente alle segnalazioni interne ed esterne, lo stesso si configura nel 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.

2.4 Misure Tecniche e informatiche per la protezione dei dati

Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni.

Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento**.** Il sistema è

installato su sistema operativo Linux su cui è attiva Full Data Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Tracciabilità

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.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati.

Controllo degli accessi logici

L'accesso applicativo Whistleblowing è consentito grazie all'esposizione dei due possibili portali di accesso, a mezzo link pubblicati sul portale istituzionale dell' Ente. Questa possibilità permette sia ai dipendenti che agli utenti esterni di accedere alle funzionalità che i portali permettono di usufruire; l'anonimato viene garantito by design, direttamente dal fornitore di servizi.

Nella gestione del processo sono presenti due possibili portali forniti dalla società GlobaLeaks; essi risultano comunque distinti nel contesto della dicitura di segnalazione, dalla quale emerge la possibilità di accedere a mezzo portale interno, cioè personalizzato con il logo e il form dell'Ente, e tramite portale esterno riferendo all'applicativo esposto sul sito dell' ANAC.

Entrambe le possibilità risultano comunque accessibili direttamente dal sito istituzionale ed entrambe idonee sia tecnicamente che proceduralmente a garantire il diritto di segnalazione.

Nella gestione delle segnalazioni il referente per la presa in carico della segnalazione ricevuta dai portali è il solo RPCT; gli accessi dell'utenza sono protetti tramite profilazione LDAP e dall'esterno mediante accesso VPN. L'accesso esterno alla piattaforma di gestione della posta elettronica viene protetto dall'autenticazione a due fattori.

Archiviazione

L'applicativo esposto sul portale fornito e gestito dalla società GlobaLeaks, implementa un database SQLite acceduto e organizzato con SQL Alchemy ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura grazie alla cifratura protetta TLS 1.2+.

Per quanto riguarda il sistema informativo dell'Ente, tutti gli applicativi gestionali, compreso il software di protocollo informatico sono dotati di sistemi di autenticazione mezzo LDAP, così come per le cartelle di rete, per differenziare correttamente le policy di accesso ai documenti. L'archiviazione del procedimento avviene a mezzo protocollazione riservata e il trattamento delle informazioni rimane circoscritto nell'ufficio dell'RPCT.

Sicurezza dei documenti cartacei

La Provincia di Parma ha la possibilità di fruire di sistemi di gestione completamente informatizzati; ciò permette di evitare, soprattutto per procedimenti ad alta riservatezza, la produzione di copie analogiche.

Minimizzazione dei dati

Essendo il sistema di trattamento dei dati completamente informatizzato, utilizzando piattaforme software centralizzate complete di sistemi di autenticazione degli utenti i dati raccolti sono "by default" minimi ed esenti da duplicazioni e ridondanze.

Gestione delle vulnerabilità tecniche

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.

A questi si aggiunge la peer review indipendente realizzata dalla comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.

Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html

Per quanto concerne la Provincia,

- sono state applicate e vengono monitorate le misure minime ICT Agid;
- é presente un sistema di monitoraggio avanzato MDR basato su EDR (End-Point Detection and Response) gestito;
- la posta elettronica gode di sistemi di sicurezza propria e se consultata dalla rete esterna è protetta da accesso a due fattori;
- i computer sono mantenuti aggiornati con sistema WSUS;
- i sistemi cloud sono certificati ed elencati in MarketPlace AGID – servizi IaaS (Infrastructure as a service).

La società GlobaLeaks dichiara alla data di valutazione dell'impatto in corso, le seguenti certificazioni abilitanti alla gestione corretta dei dati:

- Certificazioni ISO 27001 27017 27018;
- Certificazione CSA Star Level 1;
- Qualificazione ACN;
- Dichiarazione di conformità al principio DNSH;
- Dichiarazione di conformità normativa.

Backup

Per la piattaforma Whistleblowing, i sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 15 giorni necessari per finalità di disaster recovery.

Per quanto riguarda i sistemi di competenza interna all'Ente viene effettuato il backup giornaliero presso il datacenter di Lepida a Parma e una replica dei dati presso il datacenter di Lepida a Ravenna, più un'ulteriore copia presso data center dichiarato dal fornitore in Europa in compliance con la normativa GDPR.

Manutenzione

È prevista la manutenzione periodica correttiva, evolutiva e con finalità di miglioramento continuo in materia di sicurezza, realizzata con sistemi automatici o attraverso personale tecnico specializzato appositamente autorizzato.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installando gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installando gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall lato Ente è prevista una modalità di

manutenzione accessibile al solo personale dell'Ente o incaricato dall'Ente e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installando gli aggiornamenti previsti.

Sicurezza dei canali di comunicazione informatica

Tutte le connessioni dall'esterno verso la rete interna sono protette con l'autenticazione VPN sul firewall e consentite ai soli utenti autorizzati; le reti d'accesso sono controllate da sistemi di monitoraggio NOC e dagli ent point e i server sono monitorati da sistemi di sicurezza MDR.

Sicurezza dell'hardware

I datacenter dei fornitori dispongono di un'infrastruttura dotata di procedure di monitoraggio e sicurezza in accordo con la certificazione ISO27001.

Lotta contro il malware

Tutti i computer del personale addetto alla gestione del Whistleblowing e dei sub-responsabili eventualmente nominati, sono protetti da 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.

Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Per quanto riguarda l'infrastruttura di elaborazione della Provincia, sono presenti le seguenti misure di sicurezza per mitigare il rischio derivante da malware o attacchi informatici:

- Firewall perimetrale per evitare le intrusioni indesiderate dall'esterno;
- Antivirus e anti-ransomware su tutti i server e i client di rete;
- Sistema di sicurezza MDR installato su tutti i client;
- Controlli di sicurezza avanzati attuati direttamente dal fornitore sulle caselle di posta elettronica;
- Sistema di aggiornamento centralizzato WSUS per mantenere aggiornati gli End Point.

2.5 Misure organizzative per la protezione dei dati

Politica di tutela dei dati personali

La Provincia ha provveduto e periodicamente aggiorna ove necessario:

- alla designazione del Responsabile Protezione Dati (DPO), ai sensi dell'art. 37 Reg. Ue 2016/679;

- alla designazione e delega dei soggetti di cui all'art. 2 quaterdecies d.lgs. 196/2003 ai fini della nomina da parte degli stessi dei Responsabili del trattamento dei dati personali.

- limitazione al minimo degli account che hanno accesso alle informazioni di attivazione procedurale;

- limitazione dell'accessibilità al dato anche nelle successive fasi di trattamento utilizzando policy software di protezione (riservatezza documentale).

Gestione delle segnalazioni

La Provincia ha adottato e costantemente aggiorna (ultima revisione è la Determinazione Dirigenziale n. 1006 del 14/07/2023) una procedura a tutela del dipendente che segnala illeciti, che tiene conto dei contenuti del modello di procedura di gestione delle segnalazioni proposto da Whistleblowing Solutions.

Gestione del Registro delle attività di trattamento

Il Titolare del trattamento svolge una costante attività di verifica dei trattamenti effettuati e se necessario provvede all'aggiornamento del Registro delle attività di trattamento, delle Valutazioni di impatto, delle informative.

Gestione degli incidenti di sicurezza e delle violazioni dei dati

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

La Provincia con decreto presidenziale n. 230 del 5.12.18 ha approvato "la procedura per la gestione delle violazioni dei dati personali ai sensi del Regolamento Europeo 2016/679 (GDPR)".

Gestione del personale

Il Titolare del trattamento ha provveduto e provvede costantemente alla formazione dei soggetti designati/autorizzati al trattamento dei dati personali.

I soggetti designati/autorizzati al trattamento dei dati sono nominati con specifici atti, come da Regolamento provinciale e sono istruiti e formati sul corretto trattamento.

Gestione dei terzi che accedono ai dati

L'accesso ai dati da parte di terzi è legittimato da contratti, convenzioni e regolamenti. Gli accessi da parte dei terzi sono tracciati ed autorizzati dai sistemi informativi provinciali con utenze personali e a scadenza.

3. Necessità e proporzionalità del trattamento

3.1 Legittimità, liceità, necessità

I trattamenti di dati personali posti in essere dal titolare, nell'ambito della gestione del canale di segnalazione interno, sono necessari per dare attuazione agli obblighi di legge e 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 Regolamento, nonché 2-ter e 2-sexies del Codice).

3.2 Proporzionalità

In considerazione del principio di proporzionalità, i dati personali -sia del segnalante che del segnalato- sono gestiti all'interno del trattamento rispettando un approccio basato sulla minimizzazione degli stessi, in modo che siano sempre adeguati, pertinenti e limitati a quanto necessario rispetto alla finalità individuata.

4. Gestione del rischio, rischi per gli interessati e misure di contenimento

Questo capitolo svolge la valutazione dei rischi per i diritti e le libertà degli interessati, derivanti da violazioni di riservatezza, integrità e disponibilità dei dati personali trattati nei VSS alla luce delle misure tecniche ed organizzative di contenimento del rischio predisposte o in via di attuazione.

Mappa dei rischi :

Rischi **Fasi**	**Riservatezza** – violazione dovuta a divulgazione (volontaria o involontaria) non autorizzata del dato che non ne altera né modifica la sua integrità o disponibilità da parte del titolare	**Integrità** – violazione dovuta a modifica (volontaria o involontaria) non autorizzata del dato che lo altera pur non impedendone la disponibilità da parte del titolare	**Disponibilità** – violazione dovuta a indisponibilità o perdita del dato (volontaria o involontaria) che -pur non alterandone necessariamente l'integrità- lo rende non più disponibile al titolare
Trasmissione della segnalazione – il processo che inizia con la segnalazione e termina con il suo inserimento nel sistema di archiviazione delle segnalazioni	**Rischi Interni -** Malfunzionamento della piattaforma informatica; Errore di configurazione dei sistemi; Errore umano del segnalante **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione;	**Rischi Interni** Malfunzionamento della piattaforma informatica; Errore di configurazione dei sistemi; Errore umano del segnalante **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione;	**Rischi Interni** Malfunzionamento della piattaforma informatica; Crash del sistema dovuto a cause endogene Errore di configurazione dei sistemi; Errore umano del segnalante **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione; Attacco Ransomware Crash del sistema dovuto a cause esogene

Gestione della segnalazione – il processo che inizia con la comunicazione al RPCT da parte del sistema e termina con l'esito dell'istruttoria	**Rischi Interni** Malfunzionamento della piattaforma informatica; Errore di configurazione dei sistemi; Errore umano del segnalante Errore umano del RPCT/staff (incontri in sedi che non tutelano la riservatezza, Archiviazione non controllata di documenti cartacei, ecc.) **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione;	**Rischi Interni** Malfunzionamento della piattaforma informatica; Errore di configurazione dei sistemi; Errore umano del segnalante Errore umano del RPCT/staff (Archiviazione non controllata di documenti cartacei, ecc.) **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione;	**Rischi Interni** Malfunzionamento della piattaforma informatica; Crash del sistema dovuto a cause endogene Errore di configurazione dei sistemi; Errore umano del segnalante Errore umano del RPCT/staff (Archiviazione non controllata di documenti cartacei, ecc.) **Rischi Esterni** Attacco Hacker alla piattaforma informatica; Attacco Hacker alla rete dati interna; Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica; Attacco Malware o Virus attraverso diversi canali di comunicazione; Attacco Ransomware Crash del sistema dovuto a cause esogene

4.1. Gestione del rischio per gli interessati e misure di contenimento

Metodologia

Per la valutazione dei rischi si adotta la seguente metodologia.

Minacce

La valutazione dei rischi è eseguita a fronte delle seguenti minacce:

Minaccia	Descrizione
Zero	I dati degli interessati (segnalante e segnalato) sono utilizzati solo dai soggetti autorizzati, che seguono le istruzioni loro impartite; questa minaccia consente di valutare il rischio base insito nel trattamento per così come è progettato, a prescindere da comportamenti malevoli da parte di soggetti interni o esterni al processo.
Interna	I dati degli interessati (segnalante e segnalato) sono utilizzati dai soggetti autorizzati che non seguono le istruzioni loro impartite; questa minaccia consente di valutare il rischio aggiuntivo apportato da un comportamento non adeguato dei soggetti autorizzati e non impedito dalle protezioni "fin dalla progettazione e per impostazione predefinita" (art.25 GDPR) previste dal trattamento
Esterna	I dati degli interessati (segnalante e segnalato) sono utilizzati da soggetti non autorizzati, attraverso azioni tese a superare le protezioni presenti nel trattamento

Eventi

Per ogni minaccia, si identificano eventi verosimili (cioè con probabilità non completamente trascurabile) che possono comportare danni agli interessati, considerando le due principali fasi del processo (Trasmissione della segnalazione e Gestione della segnalazione) e le tre tipologie di violazioni (riservatezza, integrità, disponibilità).

Stima del danno dell'evento

Il danno ai diritti e le libertà dell'interessato conseguente all'accadimento di un evento è valutato utilizzando la seguente scala discreta di valori:

Livello	Valore	Descrizione
1	Disagio minore	Gli interessati possono andare incontro a disagi minori, che supereranno senza conseguenze di lungo periodo (perdita di tempo, rinvio di un servizio, irritazione…)
2	Disagio maggiore	Gli interessati possono andare incontro a significativi disagi, che supereranno con alcune difficoltà (costi aggiuntivi, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità...)
3	Danno superabile	Gli interessati possono andare incontro a conseguenze significative ai loro diritti e libertà individuali, che dovrebbero essere in grado di superare anche se con gravi difficoltà (perdite di denaro, danni di reputazione, danni alla proprietà, perdita del lavoro, citazione in giudizio, peggioramento della salute…)
4	Danno insuperabile	Gli interessati possono subire conseguenze significative o irreversibili ai loro diritti e libertà individuali, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte…)

Stima della probabilità dell'evento

La probabilità di accadimento di un evento è valutata utilizzando la seguente scala discreta di valori:

Livello	Valore	Descrizione
1	Improbabile	Non risulta che l'evento sia mai capitato ed il suo accadimento sorprenderebbe molto
2	Occasionale	Non si può escludere che l'evento sia accaduto in passato e che possa accadere in futuro
3	Probabile	L'evento è accaduto in passato e/o se accadesse in futuro non sorprenderebbe.
4	Frequente	L'evento è accaduto più volte.

Valutazione del rischio di un evento

Il rischio è valutato sulla base delle stime di danno e probabilità utilizzando la seguente tabella di calcolo:

4 Danno insuperabile	4 Medio	8 Alto	12 Elevato	16 Elevato
3 Danno superabile	3 Medio	6 Alto	9 Alto	12 Elevato
2 Disagio maggiore	2 Basso	4 Medio	6 Alto	8 Alto
1 Disagio minore	1 Basso	2 Basso	3 Medio	4 Medio
	1 Improbabile	2 Occasionale	3 Probabile	4 Frequente

La tabella definisce quattro possibili livelli di rischio:

Livello	Valore	Conseguenze
1-2	Basso	Il rischio è accettabile
3-4	Medio	Il rischio è accettabile e si raccomanda la ricerca ed esecuzione di ulteriori misure di riduzione
6-9	Alto	Il rischio è accettabile solo nel breve – medio periodo e deve essere affrontato con ulteriori misure di riduzione
12-16	Elevato	Il rischio richiede l'applicazione dell'art.36 GDPR.

Valutazione dei rischi e misure di contenimento

Utilizzando la metodologia precedentemente descritta, in questa sezione si procede alla valutazione del rischio per ogni minaccia / fasi del processo / violazione. Le misure evidenziate sono in corso di adozione e potranno ridurre ulteriormente il rischio.

Minaccia zero

Fase del processo	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Trasmissione Gestione	Riservatezza	Malfunzionamento della piattaforma informatica	3	1	3	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Integrità	Malfunzionamento della piattaforma informatica	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Disponibilità	Malfunzionamento della piattaforma informatica	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Disponibilità	Crash del sistema dovuto a cause endogene	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore

Minacce interne

Sono le minacce potenzialmente in capo ai soggetti attivamente coinvolti nello stesso per normativa o dalla procedura definita:

- Interessato principale (Segnalante)
- Titolare (Ente)
- Soggetto attuatore/delegato per il trattamento in oggetto (RPCT)
- Responsabili o subresponsabili esterni (gestori piattaforma e loro subresponsabili)

Fase del processo	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Trasmissione Gestione	Riservatezza	Errore di configurazione dei sistemi	3	1	3	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Integrità	Errore di configurazione dei sistemi	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Disponibilità	Errore di configurazione dei sistemi	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore

Fase del processo	Violazione	Evento	D	P	R	Nota e Misure di contenimento
Trasmissione Gestione	Riservatezza	Errore umano del segnalante	3	1	3	Formazione al personale sulle modalità di utilizzo della piattaforma
Trasmissione Gestione	Integrità	Errore umano del segnalante	1	1	1	Formazione al personale sulle modalità di utilizzo della piattaforma
Trasmissione Gestione	Disponibilità	Errore umano del segnalante	1	1	1	Formazione al personale sulle modalità di utilizzo della piattaforma
Gestione	Riservatezza	Errore umano del RPCT/staff	3	1	3	Formazione sulle modalità di utilizzo della piattaforma
Gestione	Integrità	Errore umano del RPCT/staff	1	1	1	Formazione e aggiornamento continuo del personale dell'Ente
Gestione	Disponibilità	Errore umano del RPCT/staff	1	1	1	Formazione continua del personale dell'Ente

Minacce esterne

Sono quelle potenzialmente in capo ai soggetti non attivamente coinvolti nello stesso per normativa o dalla procedura definita:

- Interessato secondario (segnalato)
- Altri soggetti, interni o esterno all'Ente, ad esclusione di quelli indicati come interni

Fase del processo	Violazione	Evento	D	P	R	Nota e misure di contenimento
Trasmissione Gestione	Riservatezza	Attacco Hacker alla piattaforma informatica	3	1	3	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Integrità	Attacco Hacker alla piattaforma informatica	3	1	3	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Disponibilità	Attacco Hacker alla piattaforma informatica	3	1	3	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore
Trasmissione Gestione	Riservatezza	Attacco Hacker alla rete dati interna	3	1	3	Misure di protezione informatiche in atto presso la Provincia
Trasmissione Gestione	Integrità	Attacco Hacker alla rete dati interna	3	1	3	Misure di protezione informatiche in atto presso la Provincia
Trasmissione Gestione	Disponibilità	Attacco Hacker alla rete dati interna	3	1	3	Misure di protezione informatiche in atto presso la Provincia
Trasmissione Gestione	Riservatezza	Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica	3	1	3	Formazione al personale sulle modalità di utilizzo della piattaforma Iniziative di awareness (consapevolezza) diffuse da parte del Servizio Informatico Procedura di gestione delle violazioni dell'Ente

Trasmissione Gestione	Integrità	Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica	3	1	3	Formazione al personale sulle modalità di utilizzo della piattaforma Iniziative di awareness (consapevolezza) diffuse da parte del Servizio Informatico Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Disponibilità	Attacco Phishing (furto di credenziali) o malware attraverso la posta elettronica	3	1	3	Formazione al personale sulle modalità di utilizzo della piattaforma Iniziative di awareness (consapevolezza) diffuse da parte del Servizio Informatico Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Riservatezza	Attacco Malware o Virus attraverso diversi canali di comunicazione	3	1	3	Misure di protezione informatiche in atto presso la Provincia e il fornitore Formazione al personale sulle modalità di utilizzo della piattaforma Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Integrità	Attacco Malware o Virus attraverso diversi canali di comunicazione	3	1	3	Misure di protezione informatiche in atto presso la Provincia e il fornitore Formazione al personale sulle modalità di utilizzo della piattaforma Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Disponibilità	Attacco Malware o Virus attraverso diversi canali di comunicazione	3	1	3	Misure di protezione informatiche in atto presso la Provincia e il fornitore Formazione al personale sulle modalità di utilizzo della piattaforma Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Disponibilità	Attacco Ransomware	3	1	3	Misure di protezione informatiche in atto presso la Provincia e il fornitore Formazione al personale sulle modalità di utilizzo della piattaforma Procedura di gestione delle violazioni dell'Ente
Trasmissione Gestione	Disponibilità	Crash del sistema dovuto a cause esogene	1	1	1	Richiesta annuale del mantenimento delle misure di protezione più aggiornate da parte del fornitore

5. Conclusioni

L'analisi del trattamento evidenzia che il trattamento dei dati personali è eseguito in conformità alla normativa vigente, è lecito e necessario ed il Titolare ha adottato misure organizzative e tecniche adeguate alla categoria e tipologia di dati trattati.

La valutazione dei rischi effettuata a partire dai risultati dell'analisi del trattamento non evidenzia rischi "elevati" per i diritti e le libertà degli interessati e le ulteriori misure tecniche ed organizzative adottate potranno ridurre i rischi residui.

Ai sensi dell'art.36.1 GDPR, il Titolare non ritiene quindi di dover consultare l'Autorità di Controllo prima di procedere al trattamento descritto nel presente documento.