WHISTLEBLOWING

DATA PROTECTION IMPACT ASSESSEMENT

Comune di Torrazza Piemonte

Città Metropolitana di Torino

29 DICEMBRE 2025

REL. 1.0

Sommario

Premessa

La Dpia – Data Protection Impact Assesment – è una procedura prevista dall'articolo 35 del Regolamento (UE) 2016/679.

La valutazione d'impatto della protezione dei dati (DPIA) serve a descrivere un trattamento di dati per valutarne la necessità, la proporzionalità e i relativi rischi.

L'obiettivo è quello di stabilire misure idonee ad affrontare i rischi in riferimento ai diritti e alle libertà delle persone fisiche di cui si effettua il trattamento dei dati.

Una DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Il Regolamento (UE) 2016/679 fa riferimento all'obbligo del titolare di tenere conto dei rischi che i trattamenti possono comportare per i diritti e le libertà delle persone:

- nell'art.24, che individua l'analisi dei rischi fra le caratteristiche dei trattamenti di cui occorre tener conto per mettere in atto tutte le misure tecniche e organizzative adeguate indicando che il Titolare deve sempre essere in grado di dimostrare di aver adottato tutte le misure necessarie affinché il trattamento sia conforme al Regolamento;
- nell'art. 35, che prevede una specifica valutazione di impatto quando i trattamenti, considerate le circostanze indicate nella norma, possono presentare rischi elevati per gli interessati, specifica i casi in cui è necessaria e procedimentalizza le modalità da seguire e gli elementi da tenere in considerazione;

  l'art.35 prevede inoltre un ruolo molto rilevante delle Autorità di controllo, che possono redigere e rendere pubblico un elenco delle tipologie di trattamenti per i quali è richiesta comunque la valutazione di impatto (art. 35, 4); così come possono, se lo ritengono opportuno, redigere un elenco delle tipologie di trattamenti per i quali essa non è necessaria.
- nell'art.36 che stabilisce la consultazione preventiva obbligatoria dell'Autorità di controllo quando il titolare ritiene che i trattamenti richiedano misure specifiche per attenuarne i rischi.

Nel concreto quindi per ogni trattamento è necessario effettuare un'analisi dei rischi (art.24) finalizzata all'accertamento del livello di rischio per poter, a valle di questa valutazione, decidere se il rischio per i cittadini sia elevato o meno e quindi se è necessario procedere con una valutazione di impatto per l'individuazione delle misure specifiche da adottare (art. 35) per minimizzare il rischio e se del caso successivamente procedere con una consultazione preventiva dell'Autorità di controllo.

Rispetto a come deve essere effettuata una DPIA è d'aiuto ricorrere a quanto indicato dal WP29[1] nelle linee guida[2] in materia di valutazione d'impatto sulla protezione dei dati personali, da cui si ricavano preziose indicazioni:

- l'analisi dei rischi relativi a un trattamento va fatta sempre prima che questo inizi;
- l'analisi va fatta rispetto a ciascun singolo trattamento, salvo il caso di trattamenti simili;

[1] Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29.

[2] Guidelines on Data Protection Impact Assessment (DPIA) (wp248rev.01) - https://ec.europa.eu/newsroom/article29/items/611236

- deve essere prestata attenzione sul piano tecnologico anche alle componenti dei dispositivi utilizzati;
- ogni analisi deve tener conto dei casi di cui all'art. 35 nonché delle specifiche indicate ai punti 71, 75 e 91 dei Considerando;
- deve essere svolta con una metodologia che tenga conto dei criteri e degli elementi indicati nell'annex 2 delle Linee guida.

Nel caso in cui al termine dell'analisi condotta secondo la metodologia indicata nelle Linee guida il titolare, sentito il DPO, ritenga che non sussistano rischi elevati può limitarsi a dare applicazione a quanto richiesto dall'art. 24.

Tuttavia, il WP29 precisa che anche in questo caso il titolare deve giustificare per iscritto le valutazioni fatte e tenere un registro dei trattamenti svolti sotto la sua responsabilità.

Quando, all'esito dell'analisi svolta nell'ambito della DPIA, risultino rischi elevati per gli interessati, il titolare deve adottare misure tecniche adeguate a minimizzare il rischio.

Le linee guida non contengono indicazioni specifiche su questo punto, in quanto aventi contenuto ed obiettivi essenzialmente procedurali; va considerato inoltre che la DPIA è un processo continuo, una valutazione che deve essere costantemente aggiornata al modificarsi delle condizioni di esercizio.

Spetta perciò al titolare individuare le misure di sicurezza o altre modalità di riduzione del rischio da adottare, sentito il DPO se nominato. Il titolare può anche consultare gli interessati o i loro rappresentanti dandone atto nel documento scritto che costituisce la parte formale della DPIA.

Nel documento è bene anche indicare i soggetti che hanno svolto l'analisi dei trattamenti e individuato le misure necessarie.

Per quanto riguarda la metodologia relativa all'individuazione delle misure idonee a diminuire i rischi, le linee guida si limitano a fissare i criteri da seguire, distinguendo tra quelle che hanno come obiettivo principale la riduzione del rischio e quelle finalizzate a dimostrare la conformità con il Regolamento.

Per quanto riguarda i casi in cui si debba consultare preventivamente l'Autorità le Linee guida indicano che il ricorso alla consultazione dell'Autorità di controllo è necessario solo quando il titolare "non riesce a individuare misure sufficienti per ridurre i rischi a un livello accettabile.

Necessità di effettuare una valutazione di impatto (DPIA) preventiva per adozione di un sistema di notifiche digitali

La DPIA è da considerarsi obbligatoria per quanto riguarda l'adozione di un sistema di Whistleblowing.

In primo luogo è da considerare il fatto che l'applicazione del Regolamento (UE) sulla protezione dei dati personali si basa sul principio di accountability che in concreto vuole dire che il regolamento pone con forza l'accento sulla "responsabilizzazione" (accountability nell'accezione inglese) di titolari e responsabili – ossia, sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in particolare, e l'intero Capo IV del regolamento). Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere

autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali – nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il primo fra tali criteri è sintetizzato dall'espressione inglese "data protection by default and by design" (si veda art. 25), ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati – tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati. Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio ("sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso", secondo quanto afferma l'art. 25(1) del regolamento) e richiede, pertanto, un'analisi preventiva e un impegno applicativo da parte dei titolari che devono sostanziarsi in una serie di attività specifiche e dimostrabili.

È quindi utile chiarire che il regolamento generale sulla protezione dei dati **non** richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche.

La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento "*possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche*" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4).

È inoltre utile precisare che il WP29[3] raccomanda di effettuare comunque la DPIA in tutti i casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

È altrettanto utile ricordare che l'articolo 35, paragrafo 3, del Regolamento (UE) 2016/679 fornisce alcuni esempi di casi nei quali un trattamento "possa presentare rischi elevati":

a) *"una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*
b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*
c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Inoltre, sempre il WP29 nelle linee guida in materia di valutazione d'impatto sulla protezione dei dati per la determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679 ha precisato che:

"come indicato dalle parole "in particolare" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati."

---

[3] Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29.

È poi necessario considerare che il Garante per la protezione dei dati personali italiano, riguardo ai criteri che un Titolare deve considerare per determinare se è necessario eseguire una valutazione di impatto (DPIA), si è espresso nel seguente modo.

"Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il regolamento 2016/679 obbliga i titolari a svolgere una valutazione di impatto prima di darvi inizio, consultando l´autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

Si tratta di uno degli elementi di maggiore rilevanza del vigente quadro normativo, perché esprime chiaramente la responsabilizzazione (accountability) dei titolari nei confronti dei trattamenti da questi effettuati.

I titolari sono infatti tenuti non soltanto a garantire l'osservanza delle disposizioni del regolamento, ma anche a dimostrare adeguatamente in che modo garantiscono tale osservanza; la valutazione di impatto ne è un esempio.

Le linee-guida[4] del WP29[5] offrono alcuni chiarimenti sul punto; in particolare, precisano quando una valutazione di impatto sia obbligatoria (oltre ai casi espressamente indicati dal regolamento all´art. 35), chi debba condurla (il titolare, coadiuvato dal responsabile della protezione dei dati, se designato), in cosa essa consista (fornendo alcuni esempi basati su schemi già collaudati in alcuni settori), e la necessità di interpretarla come un processo soggetto a revisione continua piuttosto che come un adempimento una tantum.

Le linee-guida chiariscono, peraltro, anche quando una valutazione di impatto non sia richiesta: ciò vale, in particolare, per i trattamenti in corso che siano già stati autorizzati dalle autorità competenti e non presentino modifiche significative prima del 25 maggio 2018, data di piena applicazione del regolamento.

In sostanza le linee-guida indicano che la valutazione di impatto costituisce una buona prassi al di là dei requisiti di legge, poiché attraverso di essa il titolare può ricavare indicazioni importanti e utili a prevenire incidenti futuri. In questo senso, la valutazione di impatto permette di realizzare concretamente l'altro fondamentale principio fissato nel regolamento 2016/679, ossia la protezione dei dati fin dalla fase di progettazione (data protection by design) di qualsiasi trattamento."

I criteri specifici individuati dal Gruppo Art. 29 per determinare quando la DPIA è obbligatoria sono:

- trattamenti valutativi o di scoring, compresa la profilazione;
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente; quindi, decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza) che include i trattamenti utilizzati per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o "la sorveglianza sistematica su larga scala di una zona accessibile al pubblico" (articolo 35, paragrafo 3, lettera c)). Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a

[4] 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 come modificate e adottate da ultimo il 4 ottobre 2017.

[5] Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29.

conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);

- **dati sensibili o dati aventi carattere altamente personale**, questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate in grado di aumentare il possibile rischio per i diritti e le libertà delle persone fisiche. Tali dati personali sono considerati sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico **(quali le comunicazioni elettroniche la cui riservatezza deve essere protetta)** oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione, qualora fosse previsto che i dati vengano utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, **messaggi di posta elettronica**, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;
- **trattamenti di dati personali su larga scala**, il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:
  a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
  b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
  c) la durata, ovvero la persistenza, dell'attività di trattamento;
  d) la portata geografica dell'attività di trattamento[6];
- creazione di corrispondenze o combinazione di insiemi di dati, combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio che causa un 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 in grado di opporsi e consentire 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

[6] NdR – Sempre in relazione alla popolazione di riferimento

caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

Sempre il Gruppo Art. 29 ha precisato che la DPIA non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

Conclusioni circa la necessità di effettuare la DPIA nel caso di specie

Alla luce della disamina di quanto disposto dal Regolamento (UE) 2016/679 all'articolo 35, così come interpretate dal Garante per la Protezione dei dati personali italiano e dal Gruppo dell'articolo 29 a livello europeo, appare indispensabile procedere con una Valutazione d'Impatto sulla Protezione dei Dati (DPIA). Questo passaggio diventa essenziale di fronte al potenziale alto rischio per i diritti e le libertà degli individui introdotto dall'implementazione di un sistema di whistleblowing. Data la natura di tale sistema, che coinvolge la gestione di "comunicazioni elettroniche la cui confidenzialità deve essere salvaguardata" e implica il trattamento di dati sensibili o di informazioni strettamente personali, si rientra nel criterio che contempla le categorie particolari di dati personali definite all'articolo 9 (per esempio, dettagli riguardanti le opinioni politiche) e dati personali concernenti condanne penali o reati, come specificato all'articolo 10 del Regolamento. Pertanto, si configura un'operazione di trattamento che "può comportare rischi elevati", ai sensi dell'articolo 35, comma 3, del Regolamento (UE) 2016/679.

Prendendo in considerazione i criteri definiti dal Gruppo dell'articolo 29 per determinare l'obbligatorietà della realizzazione della DPIA pare che, nel caso di specie, siano rilevabili "almeno due di questi criteri" potendosi compiere con tali servizi:

1. trattamenti di dati sensibili o dati aventi carattere altamente personale;
2. che possono comprendere anche dati relativi a interessati vulnerabili;
3. e che potrebbero comprendere utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

Inoltre 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"..

Perimetro della valutazione d'impatto

La valutazione di impatto effettuata dall'Ente in quanto titolare del trattamento prende in considerazione tutto il ciclo di vita del servizio che riguarda

1. Attivazione della Piattaforma adottata per la gestione delle segnalazioni
2. Configurazione della Piattaforma
3. Fase d'Uso della Piattaforma.
4. Fase di Dismissione della Piattaforma

Metodologia utilizzata

La valutazione d'impatto sulla protezione dei dati tiene conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto in cui il trattamento si colloca. Il concetto di rischio non si esaurisce nella considerazione delle sole violazioni o minacce alla sicurezza dei dati, ma comprende anche i possibili impatti sul piano dei diritti, delle libertà e delle legittime aspettative delle persone fisiche interessate.

La DPIA costituisce pertanto un processo strutturato e documentato, finalizzato a valutare gli aspetti tecnici e organizzativi del trattamento e a individuare misure idonee a ridurre, fino a renderli accettabili, i rischi derivanti dal trattamento stesso.

Per la realizzazione della presente DPIA è stata adottata la metodologia definita dalla CNIL, autorità francese per la protezione dei dati, utilizzando il software di supporto alla valutazione d'impatto messo a disposizione dalla medesima autorità, nella versione in lingua italiana sviluppata con la collaborazione del Garante per la protezione dei dati personali. Tale strumento fornisce un percorso guidato per la realizzazione della DPIA, conforme alle indicazioni contenute nelle linee guida del Gruppo di lavoro Articolo 29[7] in materia di valutazione d'impatto sulla protezione dei dati[8].

Il software CNIL rappresenta un ausilio metodologico e organizzativo per il titolare e consente di strutturare la valutazione secondo una sequenza logica coerente con l'articolo 35 del Regolamento UE 2016/679, includendo la descrizione sistematica del trattamento, la valutazione di necessità e proporzionalità, l'analisi dei rischi per i diritti e le libertà degli interessati e l'individuazione delle misure previste per affrontarli.

Nell'ambito della presente DPIA, la valutazione effettuata secondo la metodologia CNIL è stata integrata da un'analisi specifica del rischio con riferimento alle principali dimensioni della sicurezza del trattamento, riservatezza, integrità e disponibilità, e alle relative minacce, quali accessi illegittimi, modifiche non autorizzate, perdita o indisponibilità dei dati. Tale analisi è funzionale all'individuazione di misure tecniche e organizzative adeguate ai sensi dell'articolo 32 del Regolamento UE 2016/679.

La DPIA non è intesa come un adempimento una tantum, ma come un processo dinamico che deve essere riesaminato e aggiornato in caso di modifiche rilevanti del trattamento, delle tecnologie utilizzate, delle finalità perseguite o del livello di rischio per gli interessati.

La valutazione d'impatto è costituita dal presente documento nel suo complesso, unitamente agli allegati che ne formano parte integrante.

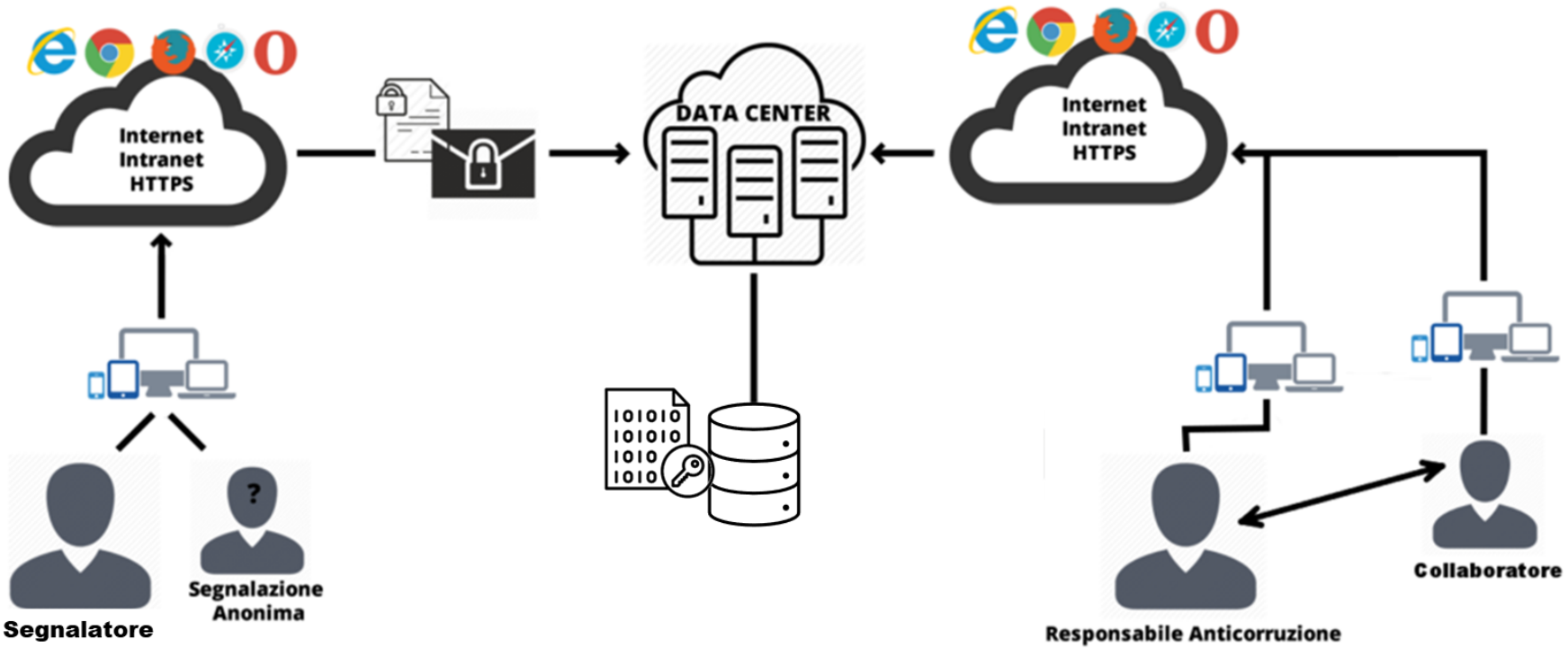
[7] Gruppo dell'articolo 29 per la tutela dei dati (in inglese Article 29 Working Party o WP29) era il gruppo di lavoro comune della autorità nazionali di vigilanza e protezione dei dati. Oggi diventato European Data Protection Board (Comitato europeo per la protezione dei dati) col nuovo Regolamento europeo ha sostituito il Gruppo di lavoro articolo 29.

[8] 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 come modificate e adottate da ultimo il 4 ottobre 2017.

Validazione

TIPOLOGIA DI APPLICAZIONE	
TIPOLOGIA	**PRESENZA**
Sistema di Gestione delle Segnalazioni di illeciti	Sì

Schema generale del sistema di gestione delle segnalazioni



Descrizione del sistema

Sistema di Gestione delle Segnalazioni di Illeciti

Il sistema di gestione delle segnalazioni di illeciti è una procedura chiave introdotta dal D.Lgs. 24/2023, che permette a chiunque acquisisca conoscenza di illeciti nell'ambito lavorativo di segnalare tali attività. Questo sistema mira a promuovere un ambiente di lavoro trasparente e giusto, proteggendo coloro che decidono di segnalare comportamenti scorretti.

Scopo della Procedura

La procedura di segnalazione degli illeciti ha l'obiettivo di facilitare la comunicazione di informazioni riguardanti violazioni individuate durante l'attività lavorativa. L'intento è di garantire una protezione efficace a chi segnala, affrontando e correggendo eventuali condotte illecite all'interno dell'ente.

Categorie di Soggetti Abilitati alla Segnalazione (Interessati)

Le segnalazioni possono essere effettuate da un'ampia gamma di soggetti, inclusi:

- Dipendenti e collaboratori
- Fornitori e subfornitori, assieme ai loro dipendenti e collaboratori
- Liberi professionisti, consulenti e lavoratori autonomi
- Volontari e tirocinanti, sia retribuiti che non
- Azionisti e figure di amministrazione o controllo
- Ex dipendenti e collaboratori
- Candidati in fase di selezione o assunzione

Protezione dei Facilitatori

La procedura estende la sua protezione anche ai soggetti facilitatori, coloro che assistono i segnalanti nel processo di segnalazione, operando all'interno dello stesso contesto lavorativo.

Oggetto delle Segnalazioni

Le segnalazioni possono includere illeciti penali, civili, amministrativi o contabili, nonché violazioni di normative comunitarie, di cui si sia venuti a conoscenza nel contesto lavorativo. Non sono comprese segnalazioni di carattere personale, che sono oggetto di altre procedure.

Gestione delle Segnalazioni

Le segnalazioni sono gestite dal Responsabile per la Prevenzione della Corruzione e la Trasparenza (RPCT), che può essere affiancato da un team di supporto. Il responsabile o l'ufficio whistleblowing si occupano della ricezione, del dialogo con il segnalante e dell'accertamento delle informazioni ricevute.

Modalità di Segnalazione

L'ente mette a disposizione come canale per le segnalazioni una piattaforma informatica crittografata per garantire la riservatezza della segnalazione e dei soggetti coinvolti.

Il segnalante per la propria segnalazione che deve essere:

- circostanziata;
- riguardante fatti riscontrabili e conosciuti direttamente dal segnalante e non riportati o riferiti da altri soggetti;
- contenente tutte le informazioni e i dati per individuare inequivocabilmente gli autori della condotta illecita.

Le segnalazioni possono essere attraverso la piattaforma https://torrazzapiemonte.segnalazioni.asmenet.it;

Trattamento delle Segnalazioni

Dopo la ricezione, il RPCT fornisce riscontri periodici al segnalante e comunica l'esito delle attività di accertamento, senza rivelare dati personali dell'eventuale soggetto segnalato.

Protezione e Riservatezza

La procedura garantisce la riservatezza dell'identità dei segnalanti, dei facilitatori e degli eventuali soggetti menzionati nella segnalazione, proteggendo le informazioni tramite strumenti tecnologici e processi organizzativi.

Tutela Contro le Ritorsioni

La procedura prevede misure specifiche per proteggere i segnalanti da qualsiasi forma di ritorsione o discriminazione a seguito della segnalazione di illeciti.

Segnalazioni Estere e Pubbliche

Il sistema prevede anche la possibilità di segnalazioni esterne all'Autorità Nazionale Anticorruzione (ANAC) in certe condizioni e stabilisce le basi per eventuali divulgazioni pubbliche, tutelando sempre l'interesse pubblico e la sicurezza del segnalante.

Per maggiori dettagli sulla procedura adottata fare rifermento alla procedura è che stata adottata con delibera di Giunta.

Descrizione della piattaforma di whistleblowing

Dal punto di vista operativo, il servizio è erogato da ASMENET Soc. Cons. a r.l., tra cui la gestione tecnica del sistema di whistleblowing, con riferimento all'esecuzione delle operazioni informatizzate di trattamento dei dati personali, relative alla raccolta, conservazione e gestione delle informazioni necessarie all'erogazione del servizio.

Architettura di sistema

L'architettura di sistema è principalmente composta da:

- Server virtualizzati su ambiente cloud sicuro Google Cloud Platform Ubuntu 24.04
- Sistema di gestione centralizzato per configurazione e monitoraggio

Software impiegato

La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.

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.

SEDI:

- **LEGALE** 21013 GALLARATE (VA) - Via Carlo Cattaneo, 9
- **OPERATIVA** 80143 NAPOLI Centro Dir. IS G1– E-mail: posta@asmel.eu – N. Verde 800 16 56 54

Vengono primariamente utilizzati le tecnologie open source:

- **Linux (Ubuntu Server)** – sistema operativo principale
- **NGINX** – reverse proxy e bilanciatore di carico
- **Python e Node.js** – gestione source code

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- Google Cloud Virtualization

Predisposizione dei sistemi virtualizzati:

- Creazione di istanze virtuali in ambiente isolato
- Deploy automatizzato tramite script di provisioning
- Replica e snapshot periodiche per il ripristino di emergenza

Architettura di rete

- Firewall hardware e software perimetrali con policy restrittive
- Connessioni cifrate (TLS/SSL) per tutte le comunicazioni di rete
- 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;
- L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Designati e Preposti al trattamento

Gli autorizzati al trattamento dati sono esclusivamente personale interno debitamente autorizzato al trattamento tramite nomina formale e istruito al trattamento dei dati.

Responsabili Esterni

- **RESPONSABILE DEL TRATTAMENTO**: ASMEL Associazione
- **SUB-RESPONSABILE DEL TRATTAMENTO**: ASMENET S.C.aR.L.

Il Sub-Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:

- ISO/IEC 27001:2017
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- ISO 9001:2015
- ISO 37001:2016
- ACN

Mappatura dei rischi

Le tre principali minacce che sono state individuate sono:

1. accesso illegittimo ai dati (riservatezza)
2. modifiche indesiderate dei dati (integrità)
3. perdita dei dati (disponibilità)

Per ogni potenziale minaccia è stata effettuata un'analisi che ha portato:

1. all'individuazione dei potenziali impatti sugli interessati che potrebbero essere prodotti al verificarsi delle minacce
2. alla stima del potenziale impatto (gravità) che il verificarsi di una determinata minaccia genererebbe
3. alla stima della probabilità che un determinata minaccia si possa verificare, ottenuta dalla pesatura della probabilità che una serie accadimenti possano verificarsi

L'impatto è classificato nel seguente modo:

IMPATTO		
Livello		Descrizione
1	Trascurabile (Lieve)	Gli interessati non subiranno alcun impatto o potrebbero incontrare qualche inconveniente, superabile senza difficoltà
2	Limitato (Medio)	Gli interessati potrebbero sperimentare inconvenienti significativi, superabili nonostante alcune difficoltà.
3	Importante (Grave)	Gli interessati potrebbero subire conseguenze significative, che dovrebbero essere in grado di superare, ma con difficoltà reali e significative
4	Massimo (Gravissimo)	Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

La probabilità è classificata nel seguente modo:

PROBABILITA'		
Livello		Descrizione
1	Trascurabile (Improbabile)	Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
2	Limitato (Poco probabile)	Appare difficile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
3	Importante (Probabile)	Appare possibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti
4	Massimo (Altamente proba	Appare estremamente facile per le fonti di rischio considerate concretizzare una minaccia basandosi sulle caratteristiche dei supporti

Il rischio è classificato nel seguente modo:

RISCHIO		
Livello		Descrizione
1-2	Basso	Il rischio può essere considerato di livello basso
3-4	Medio	Il rischio può essere considerato di livello medio
5-8	Alto	Il rischio può essere considerato di livello alto
9-16	Altissimo	Il rischio può essere considerato di livello altissimo

Il livello di rischio è calcolato con la seguente formula:

RISCHIO = IMPATTO * PROBABILITA'

Una volta calcolato il rischio iniziale è stato effettuato il calcolo del rischio residuo calcolando la forza di mitigazione che hanno le misure di mitigazione in essere per il trattamento preso in considerazione attraverso la pesatura di ogni singola misura sia per quanto riguarda la mitigazione dell'impatto sia per quanto riguarda la mitigazione della probabilità.

Di seguito vengono illustrati i singoli passaggi effettuati per il calcolo del rischio.

Mappatura dei rischi

Accesso illegittimo ai dati	Mitigazione Impatto (Gravità)	Mitigazione Probabilità
	Misure organizzative	**Misure organizzative**
Gravità: Limitato (Medio)	+ Procedure per l'utilizzo delle notifiche digitali	+ Procedure per l'utilizzo delle notifiche digitali
Probabilità: Importante (Probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Alto	+ Informativa	~~- Informativa~~
	+ Esercizio dei diritti degli interessati	+ Esercizio dei diritti degli interessati
Impatti potenziali	+ Tracciabilità	+ Tracciabilità
+ comunicazione dei dati non autorizzata	+ Archiviazione	+ Archiviazione
+ diffusione dei dati non autorizzata	+ Minimizzazione dei dati	+ Minimizzazione dei dati
~~- notifica dell'atto ad altra persona~~	+ Manutenzione	+ Manutenzione
~~- mancata notifica di un atto~~	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile d	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
	+ Anonimizzazione	+ Anonimizzazione
Accadimenti	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ malware	+ Formazione continua	+ Formazione continua
+ hacker	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ furto del dispositivo	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
~~- cancellazione involontaria~~	+ Lotta contro il malware	+ Lotta contro il malware
~~- cancellazione volontaria~~	+ Certificazioni sulla sicurezza delle informazioni	+ Certificazioni sulla sicurezza delle informazioni
~~- distruzione del dispositivo~~	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
Fonti	+ Gestione dei rischi	+ Gestione dei rischi
+ fonte umana esterna	**Misure tecniche**	**Misure tecniche**
+ fonte umana interna	+ Crittografia	+ Crittografia
~~- fonte non umana~~	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'applicazione web	+ Sicurezza dell'applicazione web
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Vulnerabilità	+ Vulnerabilità
	~~- Backup~~	~~- Backup~~

Modifiche indesiderate ai dati	Mitigazione Impatto (Gravità)	Mitigazione Probabilità
Gravità: Limitato (Medio)	Misure organizzative	Misure organizzative
Probabilità: Importante (Probabile)	+ Procedure per l'utilizzo delle notifiche digitali	+ Procedure per l'utilizzo delle notifiche digitali
Rischio: Alto	+ Registro dei trattamenti	+ Registro dei trattamenti
	~~- Informativa~~	~~- Informativa~~
	~~- Esercizio dei diritti degli interessati~~	~~- Esercizio dei diritti degli interessati~~
Impatti potenziali	+ Tracciabilità	+ Tracciabilità
~~- comunicazione dei dati non autorizzata~~	+ Archiviazione	+ Archiviazione
~~- diffusione dei dati non autorizzata~~	+ Minimizzazione dei dati	+ Minimizzazione dei dati
+ notifica dell'atto ad altra persona	+ Manutenzione	+ Manutenzione
+ mancata notifica di un atto	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile d	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
	+ Anonimizzazione	+ Anonimizzazione
Accadimenti	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ malware	+ Formazione continua	+ Formazione continua
+ hacker	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ furto del dispositivo	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
~~- cancellazione involontaria~~	+ Lotta contro il malware	+ Lotta contro il malware
~~- cancellazione volontaria~~	+ Certificazioni sulla sicurezza delle informazioni	+ Certificazioni sulla sicurezza delle informazioni
~~- distruzione del dispositivo~~	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
Fonti	+ Gestione dei rischi	+ Gestione dei rischi
+ fonte umana esterna	Misure tecniche	Misure tecniche
+ fonte umana interna	+ Crittografia	+ Crittografia
~~- fonte non umana~~	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'applicazione web	+ Sicurezza dell'applicazione web
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Vulnerabilità	+ Vulnerabilità
	+ Backup	~~- Backup~~

Perdita dei dati	Mitigazione Impatto (Gravità)	Mitigazione Probabilità
	Misure organizzative	**Misure organizzative**
Gravità: Trascurabile (Lieve)	+ Procedure per l'utilizzo delle notifiche digitali	+ Procedure per l'utilizzo delle notifiche digitali
Probabilità: Massimo (Altamente probabile)	+ Registro dei trattamenti	+ Registro dei trattamenti
Rischio: Medio	- Informativa	- Informativa
	- Esercizio dei diritti degli interessati	- Esercizio dei diritti degli interessati
Impatti potenziali	+ Tracciabilità	+ Tracciabilità
- comunicazione dei dati non autorizzata	+ Archiviazione	+ Archiviazione
- diffusione dei dati non autorizzata	+ Minimizzazione dei dati	+ Minimizzazione dei dati
- notifica dell'atto ad altra persona	+ Manutenzione	+ Manutenzione
+ mancata notifica di un atto	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile d	+ Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
	+ Anonimizzazione	+ Anonimizzazione
Accadimenti	+ Politica di tutela della privacy	+ Politica di tutela della privacy
+ malware	+ Formazione continua	+ Formazione continua
+ hacker	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali	+ Gestire gli incidenti di sicurezza e le violazioni dei dati personali
+ furto del dispositivo	+ Vigilanza sulla protezione dei dati	+ Vigilanza sulla protezione dei dati
+ cancellazione involontaria	+ Lotta contro il malware	+ Lotta contro il malware
+ cancellazione volontaria	+ Certificazioni sulla sicurezza delle informazioni	+ Certificazioni sulla sicurezza delle informazioni
+ distruzione del dispositivo	+ Prevenzione delle fonti di rischio	+ Prevenzione delle fonti di rischio
Fonti	+ Gestione dei rischi	+ Gestione dei rischi
+ fonte umana esterna	**Misure tecniche**	**Misure tecniche**
+ fonte umana interna	- Crittografia	+ Crittografia
+ fonte non umana	+ Controllo degli accessi logici	+ Controllo degli accessi logici
	+ Sicurezza dell'applicazione web	+ Sicurezza dell'applicazione web
	+ Gestione postazioni	+ Gestione postazioni
	+ Sicurezza dei canali informatici	+ Sicurezza dei canali informatici
	+ Sicurezza dell'hardware	+ Sicurezza dell'hardware
	+ Vulnerabilità	+ Vulnerabilità
	+ Backup	+ Backup

Panoramica delle misure tecniche ed organizzative

Nella schematizzazione che segue sono riportate in forma sintetica:

- i principi fondamentali su cui si basano le misure tecniche e organizzative che sono state adottate al fine di minimizzare il rischio;
- le misure tecniche e organizzative che sono state adottate;
- i rischi che sono stati individuati.

	Principi fondamentali	
	Reg. UE 2016/69	Principi
1	Adeguata	Finalità
2	Adeguata	Basi legali
3	Adeguata	Adeguatezza dei dati
4	Adeguata	Esattezza dei dati
5	Adeguata	Periodo di conservazione
6	Adeguata	Informativa
7	Adeguata	Raccolta del consenso
8	Adeguata	Diritto di accesso
9	--	Diritto alla portabilità dei dati
10	Adeguata	Diritto di rettifica
11	Adeguata	Diritto di cancellazione
12	Adeguata	Diritto di limitazione
13	--	Diritto di opposizione
14	Adeguata	Responsabili del trattamento
15	Adeguata	Trasferimento dei dati

	Misure tecniche esistenti		
	Reg. UE 2016/69	**D.lgs. 51/2018**	Misure
1	Adeguata	Adeguata	Procedure per l'utilizzo delle notifiche digitali
2	Adeguata	Adeguata	Registro dei trattamenti
3	Adeguata	Adeguata	Informativa
4	Adeguata	Adeguata	Esercizio dei diritti degli interessati
5	Adeguata	Adeguata	Tracciabilità
6	Adeguata	Adeguata	Archiviazione
7	Adeguata	Adeguata	Minimizzazione dei dati
8	Adeguata	Adeguata	Manutenzione
9	Adeguata	Adeguata	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)
10	Adeguata	Adeguata	Anonimizzazione
11	Adeguata	Adeguata	Politica di tutela della privacy
12	Adeguata	Adeguata	Formazione continua
13	Adeguata	Adeguata	Gestire gli incidenti di sicurezza e le violazioni dei dati personali
14	Adeguata	Adeguata	Vigilanza sulla protezione dei dati
15	Adeguata	Adeguata	Lotta contro il malware
16	Adeguata	Adeguata	Certificazioni sulla sicurezza delle informazioni
17	Adeguata	Adeguata	Prevenzione delle fonti di rischio
18	Adeguata	Adeguata	Gestione dei rischi
19	Adeguata	Adeguata	Crittografia
20	Adeguata	Adeguata	Controllo degli accessi logici
21	Adeguata	Adeguata	Gestione postazioni
22	Adeguata	Adeguata	Sicurezza dei canali informatici
23	Adeguata	Adeguata	Sicurezza dell'hardware
24	Adeguata	Adeguata	Sicurezza dell'applicazione web
25	Adeguata	Adeguata	Vulnerabilità
26	Adeguata	Adeguata	Backup

Legenda	
Adeguata	La misura è stata valutata sufficiente
Da implementare	La misura è assente o per come applicata non è ritenuta adeguata e quindi deve essere implementata
--	La misura è considerata non applicabile in relazione alle specifiche condizioni in cui viene effettuato il trattamento

Calcolo del rischio

CALCOLO DEL RISCHIO								
		Peso	Accesso Illegittimo		Modifiche		Perdita dei dati	
Impatto	**Impatti potenziali**	**4**		**2**		**2**		**1**
	comunicazione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	diffusione dei dati non autorizzata	25,00%	1	1,00		0,00		0,00
	notifica dell'atto ad altra persona	25,00%		0,00	1	1,00		0,00
	mancata notifica di un atto	25,00%		0,00	1	1,00	1	1,00
Probabilità		**4**		**2,9**		**2,9**		**4**
	Accadimenti	**3**		**2,1**		**2,1**		**3**
	malware	25,00%	1	0,75	1	0,75	1	0,75
	hacker	25,00%	1	0,75	1	0,75	1	0,75
	furto del dispositivo	20,00%	1	0,60	1	0,60	1	0,60
	cancellazione involontaria	10,00%		0,00		0,00	1	0,30
	cancellazione volontaria	10,00%		0,00		0,00	1	0,30
	distruzione del dispositivo	10,00%		0,00		0,00	1	0,30
	Fonti	**1**		**0,8**		**0,8**		**1**
	fonte umana esterna	40,00%	1	0,40	1	0,40	1	0,40
	fonte umana interna	40,00%	1	0,40	1	0,40	1	0,40
	fonte non umana	20,00%		0,00		0,00	1	0,20
Mitigazione Impatto (Gravità)	*Valore di mitigazione**	**3,00**	**1,5**	**1,38**	**1,5**	**1,38**	**0,75**	**0,66**
	Percentuale di rischio residuo		28,13%	31%	30,56%	31%	33,68%	34%
	Misure organizzative	**2,00**	**1**	**0,94**	**1**	**0,88**	**0,5**	**0,44**
	Procedure per l'utilizzo delle notifiche digitali	25,00%	1	0,25	1	0,25	1	0,13
	Registro dei trattamenti	2,94%	1	0,03	1	0,03	1	0,01
	Informativa	2,94%	1	0,03		0,00		0,00
	Esercizio dei diritti degli interessati	2,94%	1	0,03		0,00		0,00
	Tracciabilità	2,94%	1	0,03	1	0,03	1	0,01
	Archiviazione	2,94%	1	0,03	1	0,03	1	0,01
	Minimizzazione dei dati	2,94%	1	0,03	1	0,03	1	0,01
	Manutenzione	2,94%	1	0,03	1	0,03	1	0,01
	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)	25,00%	1	0,25	1	0,25	1	0,13
	Anonimizzazione	2,94%	1	0,03	1	0,03	1	0,01
	Politica di tutela della privacy	2,94%	1	0,03	1	0,03	1	0,01
	Formazione continua	2,94%	1	0,03	1	0,03	1	0,01
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	2,94%	1	0,03	1	0,03	1	0,01
	Vigilanza sulla protezione dei dati	2,94%	1	0,03	1	0,03	1	0,01
	Lotta contro il malware	2,94%	1	0,03	1	0,03	1	0,01
	Certificazioni sulla sicurezza delle informazioni	2,94%	1	0,03	1	0,03	1	0,01
	Prevenzione delle fonti di rischio	2,94%	1	0,03	1	0,03	1	0,01
	Gestione dei rischi	2,94%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1,00**	**0,5**	**0,44**	**0,5**	**0,50**	**0,25**	**0,22**
	Crittografia	12,50%	1	0,06	1	0,06		0,00
	Controllo degli accessi logici	12,50%	1	0,06	1	0,06	1	0,03
	Gestione postazioni	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dei canali informatici	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'hardware	12,50%	1	0,06	1	0,06	1	0,03
	Sicurezza dell'applicazione web	12,50%	1	0,06	1	0,06	1	0,03
	Vulnerabilità	12,50%	1	0,06	1	0,06	1	0,03
	Backup	12,50%		0,00	1	0,06	1	0,03
Mitigazione Probabilità	*Valore di mitigazione**	**3,00**	**2,175**	**1,96**	**2,175**	**1,91**	**3**	**2,76**
	Percentuale di rischio residuo		30,90%	33%	33,68%	34%	30,56%	31%
	Misure organizzative	**2,00**	**1,45**	**1,32**	**1,45**	**1,28**	**2**	**1,76**
	Procedure per l'utilizzo delle notifiche digitali	25,00%	1	0,36	1	0,36	1	0,50
	Registro dei trattamenti	2,94%	1	0,04	1	0,04	1	0,06
	Informativa	2,94%		0,00		0,00		0,00
	Esercizio dei diritti degli interessati	2,94%	1	0,04		0,00		0,00
	Tracciabilità	2,94%	1	0,04	1	0,04	1	0,06
	Archiviazione	2,94%	1	0,04	1	0,04	1	0,06
	Minimizzazione dei dati	2,94%	1	0,04	1	0,04	1	0,06
	Manutenzione	2,94%	1	0,04	1	0,04	1	0,06
	Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)	25,00%	1	0,36	1	0,36	1	0,50
	Anonimizzazione	2,94%	1	0,04	1	0,04	1	0,06
	Politica di tutela della privacy	2,94%	1	0,04	1	0,04	1	0,06
	Formazione continua	2,94%	1	0,04	1	0,04	1	0,06
	Gestire gli incidenti di sicurezza e le violazioni dei dati personali	2,94%	1	0,04	1	0,04	1	0,06
	Vigilanza sulla protezione dei dati	2,94%	1	0,04	1	0,04	1	0,06
	Lotta contro il malware	2,94%	1	0,04	1	0,04	1	0,06
	Certificazioni sulla sicurezza delle informazioni	2,94%	1	0,04	1	0,04	1	0,06
	Prevenzione delle fonti di rischio	2,94%	1	0,04	1	0,04	1	0,06
	Gestione dei rischi	2,94%	1	0,00	1	0,00	1	0,00
	Misure tecniche	**1**	**0,725**	**0,63**	**0,725**	**0,63**	**1**	**1,00**
	Crittografia	12,50%	1	0,09	1	0,09	1	0,13
	Controllo degli accessi logici	12,50%	1	0,09	1	0,09	1	0,13
	Gestione postazioni	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dei canali informatici	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'hardware	12,50%	1	0,09	1	0,09	1	0,13
	Sicurezza dell'applicazione web	12,50%	1	0,09	1	0,09	1	0,13
	Vulnerabilità	12,50%	1	0,09	1	0,09	1	0,13
	Backup	12,50%		0,00		0,00	1	0,13

* Viene sempre matenuta una percentuale del 25% che non è mitigabile (viene usato come fondo scala 3 anziché 4)

Rischio originario

RISCHIO ORIGINARARIO				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Integrità	Modifiche indesiderate	**2,00** Limitato (Medio)	**3,00** Importante (Probabile)	**6,00** Alto
Disponibilità	Perdita di dati	**1,00** Trascurabile (Lieve)	**4,00** Massimo (Altamente probabile)	**4,00** Medio

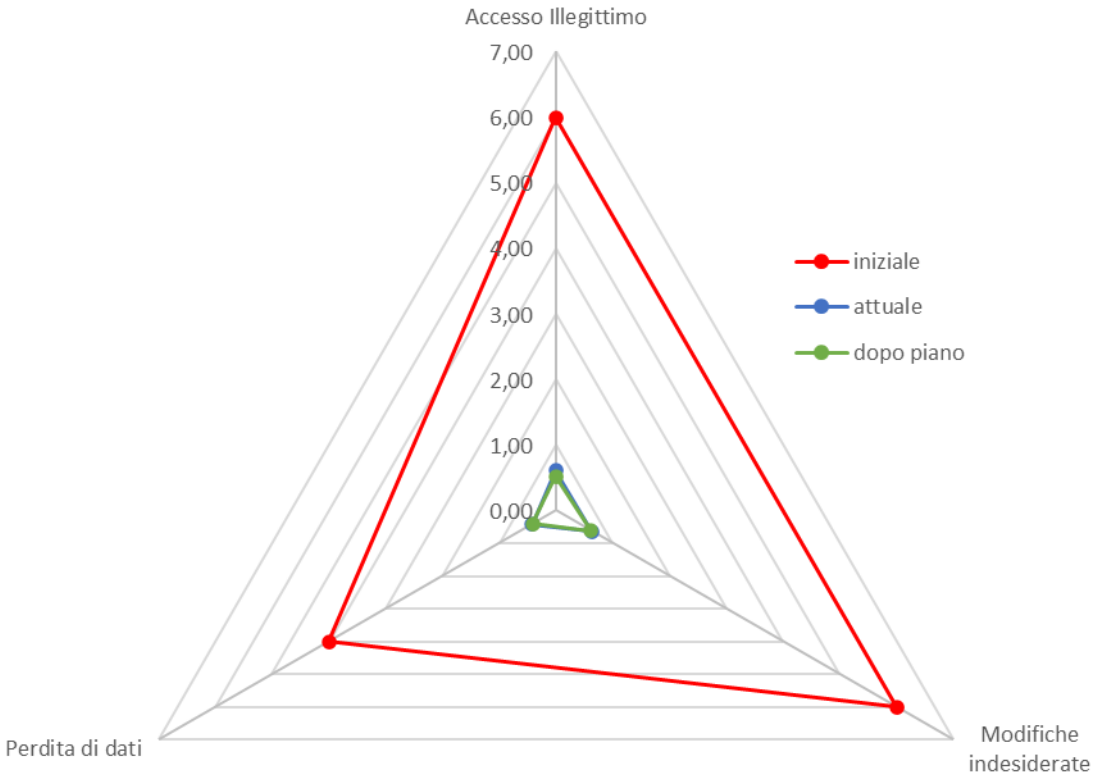
Rischio mitigato con le misure tecniche ed organizzative già adottate

RISCHIO RESIDUO ALLO STATO DELLE COSE (ATTUALE) - DOPO APPLICAZIONE MISURE DI MITIGAZIONE				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**0,62** Trascurabile (Lieve)	**0,98** Trascurabile (Improbabile)	**0,61** Basso
Integrità	Modifiche indesiderate	**0,62** Trascurabile (Lieve)	**1,02** Limitato (Poco probabile)	**0,63** Basso
Disponibiltà	Perdita di dati	**0,34** Trascurabile (Lieve)	**1,24** Limitato (Poco probabile)	**0,42** Basso

Rischio mitigato con le misure tecniche ed organizzative previste dal piano di azione

RISCHIO RESIDUO DOPO L'ATTUAZIONE DELLE PIANO DI AZIONE				
AREA DI IMPATTO	MINACCIA	GRAVITA'	PROBABILITA'	RISCHIO
Riservatezza	Accesso Illegittimo	**0,56** Trascurabile (Lieve)	**0,93** Trascurabile (Improbabile)	**0,52** Basso
Integrità	Modifiche indesiderate	**0,61** Trascurabile (Lieve)	**1,01** Limitato (Poco probabile)	**0,62** Basso
Disponibiltà	Perdita di dati	**0,34** Trascurabile (Lieve)	**1,22** Limitato (Poco probabile)	**0,41** Basso

Effetto delle misure tecniche ed organizzative sul rischio



	iniziale	attuale	dopo piano
Accesso Illegittimo	**6,00** Alto	**0,61** Basso	**0,52** Basso
Modifiche indesiderate	**6,00** Alto	**0,63** Basso	**0,62** Basso
Perdita di dati	**4,00** Medio	**0,42** Basso	**0,41** Basso

Piano d'azione

Principi fondamentali

Rispetto ai principi fondamentali che sono stati presi in considerazione non si prevede un piano di azione per adottarne di ulteriori, in quanto quelli considerati si ritengono coerenti e adeguati al trattamento in oggetto.

Misure consigliate / da pianificate

In relazione al servizio di segnalazione degli illeciti, noto come whistleblowing, si constata che le misure tecniche e organizzative attualmente adottate risultano ADEGUATE al trattamento dati previsto, delineando un profilo di rischio QUALIFICATO COME BASSO.

Si raccomanda di conformarsi pienamente alle prescrizioni del D.Lgs. 24/2023, emesso in attuazione della Direttiva (UE) 2019/1937.

Nessuno specifico piano d’azione è indicato.

Rischi

Non si prevedono rischi ulteriori che potrebbero presentarsi nel tempo al variare delle condizioni.

Parere del Tecnico che ha effettuato la valutazione, del DPO e degli interessati

Indicazioni del tecnico che ha supportato il Titolare nella realizzazione della valutazione

Si precisa che la valutazione è stata effettuata sulla base dei dati raccolti direttamente e/o forniti dal personale e dai tecnici incaricati dall'Ente.

Tutti i dati si riferiscono a elementi funzionanti, disponibili e/o configurati sul sistema durante il periodo di osservazione.

L'analisi non ha lo scopo di valutare cause di guasti e/o malfunzionamenti.

Il documento riprende i caratteri generali dell'architettura e della configurazione del sistema, senza entrare nel dettaglio delle singole configurazioni delle componenti attive.

La valutazione ha preso in considerazione i seguenti aspetti:

- la natura, la portata, lo scopo e il contesto del trattamento: il trattamento dei dati personali avviene nell'ambito del servizio di segnalazione degli illeciti, noto come whistleblowing, che consente a dipendenti, collaboratori o anche a terze parti di segnalare in modo sicuro e protetto eventuali comportamenti illeciti o violazioni delle norme all'interno di un'organizzazione, sia essa pubblica o privata;
- i rischi per i diritti e le libertà delle persone fisiche: i rischi per i diritti e le libertà delle persone fisiche sono legati alla possibilità di accesso non autorizzato ai dati personali, alla possibilità di uso improprio dei dati personali e alla possibilità di perdita dei dati personali;
- le misure di mitigazione dei rischi: le misure di mitigazione dei rischi adottate nel complesso includono misure di sicurezza tecniche e organizzative, quali ad esempio l'utilizzo di crittografia, l'autenticazione a due fattori e l'accesso controllato ai dati personali;

La valutazione ha concluso che il servizio nel complesso rispetta i principi di protezione dei dati personali e che le misure di mitigazione dei rischi adottate sono adeguate a garantire la sicurezza dei dati personali.

La valutazione DPIA ha evidenziato alcuni rischi, quali:

- il rischio di accesso non autorizzato ai dati personali;
- il rischio di perdita o distruzione dei dati personali;
- Il rischio di diffusione dei dati personali a terzi non autorizzati.

Per mitigare questi rischi, i due servizi, tra le altre, adottano le seguenti misure:

- i dati personali sono conservati in un ambiente sicuro e protetto;
- l'accesso ai dati personali è consentito solo a personale autorizzato;
- i dati personali sono protetti da misure di sicurezza tecniche e organizzative.

Nella valutazione sono stati considerati anche i benefici derivanti dall'utilizzo di sistemi di gestione delle segnalazioni degli illeciti.

L’analisi ha evidenziato che tali sistemi non solo migliorano l'efficienza e l'efficacia nella gestione delle segnalazioni di illeciti, ma contribuiscono anche alla creazione di un ambiente lavorativo etico e trasparente.

Ecco alcuni dei principali vantaggi:

- Miglioramento della Conformità Normativa: un sistema informatizzato aiuta a garantire che l'organizzazione rispetti le leggi nazionali e internazionali in materia di whistleblowing, riducendo il rischio di sanzioni legali e finanziarie.
- Rafforzamento della Cultura Aziendale: la presenza di un meccanismo di segnalazione trasparente e sicuro promuove una cultura di integrità e responsabilità, incoraggiando i dipendenti a esprimersi in caso di comportamenti illeciti senza timore di ritorsioni.
- Prevenzione e Rilevamento Precoce di Illeciti: grazie alla possibilità di segnalare tempestivamente azioni sospette o non etiche, l'organizzazione può intervenire rapidamente per indagare e risolvere i problemi, prevenendo danni maggiori.
- Miglioramento della Gestione del Rischio: un sistema di whistleblowing ben strutturato permette di identificare e gestire proattivamente i rischi legati a frodi, corruzione, violazioni legali e altri illeciti, proteggendo così la reputazione e gli asset dell'organizzazione.
- Riduzione dei Costi: la prevenzione e il rilevamento precoce di frodi o altre attività illecite possono risultare in un significativo risparmio di costi legati a perdite finanziarie, sanzioni legali e danni reputazionali.
- Trasparenza e Fiducia: un sistema informatizzato sicuro per il whistleblowing aumenta la trasparenza delle operazioni aziendali e rafforza la fiducia dei dipendenti, dei clienti, dei fornitori e di altre parti interessate.
- Efficienza Operativa: la digitalizzazione del processo di segnalazione semplifica la gestione delle segnalazioni, consentendo un trattamento più rapido e organizzato delle stesse e una migliore allocazione delle risorse per le indagini.
- Supporto alla Decisione: i dati raccolti tramite il sistema di whistleblowing possono fornire spunti preziosi per il processo decisionale strategico e per il miglioramento continuo delle politiche e delle procedure interne.

L'adozione di un sistema informatizzato per la gestione del whistleblowing può portare quindi portare a un miglioramento significativo nella gestione dei rischi, nella conformità normativa, nella cultura dell’Ente e nella reputazione complessiva dell'organizzazione.

Nell'ambito del **servizio di gestione delle segnalazioni di illeciti, noto come whistleblowing**, la valutazione conclusiva evidenzia che, nonostante il trattamento dati intrinseco rappresenti un rischio elevato per i diritti e le libertà dei soggetti coinvolti, le misure tecniche e organizzative attualmente impiegate, arricchite da procedure operative specifiche e obbligatorie per il personale addetto, risultano efficaci nel mitigare tali rischi. Di conseguenza, **il RISCHIO RESIDUALE è ridotto a un livello considerabile come BASSO**.

Nome del DPO/RPD

iSimply Srl (Dott. Enrico CAPIRONE)
Via Palestro, 45 - 10015 Ivrea (To)
e-mail dpo@isimply.it
telefono +39 0125 1899500

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD sul trattamento dei dati nel servizio di segnalazione degli illeciti:

Si considera che il trattamento dati previsto dal servizio di gestione delle segnalazioni degli illeciti possa essere implementato perché le misure tecniche e organizzative attualmente adottate, insieme alle procedure operative dettagliate e vincolanti per gli operatori autorizzati, sono adeguate a mitigare efficacemente il rischio.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si ritiene utile per questo trattamento di richiedere il parere degli interessati in quanto è un trattamento finalizzato a semplificare la comunicazione dei segnalanti di quelle segnalazioni che riguardano comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, attuato nel pieno rispetto della normativa e con modalità analoga a quanto già effettuato in numerosissimi contesti simili.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

I dati personali trattati sono i seguenti:

- Dati di registrazione

  Dati identificativi e di contatto del referente del Titolare che attiva il servizio di digital whistleblowing (RPCT).

- Categorie particolari di dati

  Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

- Dati relativi a condanne penali e reati

  Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

I dati personali sono trattati per la finalità di individuare comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato e che possono consistere in:

- illeciti amministrativi, contabili, civili o penali;
- condotte illecite rilevanti ai sensi del decreto legislativo 231/2001, o violazioni dei modelli di organizzazione e gestione ivi previsti;
- illeciti che rientrano nell'ambito di applicazione degli atti dell'Unione europea o nazionali relativi ai seguenti settori: appalti pubblici; servizi, prodotti e mercati finanziari e prevenzione del riciclaggio e del finanziamento del terrorismo; sicurezza e conformità dei prodotti; sicurezza dei trasporti; tutela dell'ambiente; radioprotezione e sicurezza nucleare; sicurezza degli alimenti e dei mangimi e salute e benessere degli animali; salute pubblica; protezione dei consumatori; tutela della vita privata e protezione dei dati personali e sicurezza delle reti e dei sistemi informativi;
- atti od omissioni che ledono gli interessi finanziari dell'Unione;
- atti od omissioni riguardanti il mercato interno;
- atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni di cui agli atti dell'Unione.

Quali sono le responsabilità connesse al trattamento?

Il titolare è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa, sia nazionale che internazionale, in materia di protezione dei dati personali. Nello specifico gli obblighi sono:

- trattamento dei dati in modo lecito, corretto e trasparente nei confronti dell'interessato;
- divieto di trattamento dei dati ex art. 9 tranne nei casi di esenzione;
- informare correttamente e in maniera trasparente gli interessati;
- garantire il rispetto dei diritti degli interessati;

- adottare le misure tecniche e organizzative adeguate a garantire, sin dalla fase della progettazione e per impostazione predefinita (privacy by design e by default), la tutela dei diritti dell'interessato e per garantire che i dati non siano persi, alterati, distrutti o comunque trattati illecitamente;
- vincolo al dovere di riservatezza dei dati, inteso come dovere di non usare, comunicare o diffondere i dati al di fuori del trattamento;
- fornire le istruzioni al responsabile del trattamento;
- tenere il registro dei trattamenti;
- fornire le istruzioni e formare il personale;
- documentare la violazione dei dati personali, notificarle al Garante e comunicarle agli interessati nei casi previsti;
- cooperare con l'autorità di controllo quando richiesto;
- redigere le valutazioni di impatto nei casi previsti;
- nominare il DPO.

Più in generale il Titolare del trattamento è soggetto alle seguenti norme di riferimento:

Norma	Titolo della fonte	Descrizione
Direttiva (UE) 2019/1937	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	Dispone in merito alla protezione delle persone che segnalano comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato
D.Lgs. 24/2023	DECRETO LEGISLATIVO 10 marzo 2023, n. 24 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.	Dispone in merito alla protezione delle persone che segnalano comportamenti, atti od omissioni che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato
D.Lgs. 231/2001	DECRETO LEGISLATIVO 8 giugno 2001, n. 231 Disciplina della responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni anche prive di personalità giuridica, a norma dell'articolo 11 della legge 29 settembre 2000, n. 300.	Dispone in merito alla responsabilità amministrativa da reato
D.Lgs. 196/2003	Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE	Norma nazionale di riferimento per quanto riguarda il trattamento dei dati personali.
Direttiva (UE) 2016/680	Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio;	Norma UE (direttiva) di riferimento per quanto riguarda il trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali.
D.Lgs. 51/2018	Decreto Legislativo 18 maggio 2018, n. 51 – Attuazione della Direttiva UE 2016/680 relativa "alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che	Norma nazionale di adattamento della direttiva UE per quanto riguarda il trattamento dei dati personali.

Norma	Titolo della fonte	Descrizione
	abroga la decisione quadro 2008/977/GAI del Consiglio”;	
DPR del 15/01/2018	Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia". *L’art. 57 del D.Lgs. 196/2013 è stato abrogato a decorrere dall’8 giugno 2019, dall’art. 49, comma 2, del D.Lgs. 51/208, ma ha ripreso vigenza dal 15 giugno 2019 fino al 31 dicembre 2019. NON PIU’ IN VIGORE.*	Regolamento sulle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia.

Ci sono standard applicabili al trattamento?

L’utilizzo dei sistemi di notifica digitale viene attuato attraverso un corretto impiego delle applicazioni e nel rispetto dei principi applicabili al trattamento di dati personali di cui all’art. 5 dell’RGPD:

1. liceità, quale rispetto della normativa: il trattamento di dati personali effettuato da parte di soggetti pubblici per lo svolgimento delle funzioni istituzionali. Esso, infatti, è necessario per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui i Comuni sono investiti.
2. proporzionalità, con sistemi attuati con attenta valutazione: nel commisurare la necessità dell’adozione del servizio di notifiche digitali al grado di rischio concreto, si sono considerati i benefici prodotti dall'aumento dell'efficienza e dell'efficacia delle notifiche degli atti della pubblica amministrazione, la significativa riduzione dei costi delle notifiche degli atti della pubblica amministrazione, l'aumento della trasparenza e della tracciabilità delle notifiche degli atti della pubblica amministrazione;
3. finalità, attuando il trattamento dei dati solo per scopi determinati ed espliciti: per fini istituzionali che non richiedano prestazioni di elaborazioni aggiuntive inviare comunicazioni a valore legale verso persone fisiche e giuridiche nel perimetro dell'art. 26 DL 76/2020 quindi consentire l'invio e la gestione delle notifiche digitali degli atti della pubblica amministrazione garantendo la sicurezza e la riservatezza dei dati personali;
4. necessità, con esclusione di uso superfluo del servizio: i sistemi sono configurati per fare in modo che i dati personali raccolti siano limitati a quelli strettamente necessari per le finalità del trattamento che non siano utilizzati per finalità diverse da quelle per le quali sono stati raccolti e siano conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Inoltre, ai sensi del Art. 32 del RGPD, per effettuare il trattamento devono essere adottate misure tecniche ed organizzative adeguate a garantire un livello di sicurezza proporzionato al rischio, lo stesso articolo fissa alcuni principi fondamentali. In particolare, le misure di sicurezza devono essere approntate tenendo conto dei seguenti criteri:

1. lo stato dell’arte;
2. i costi di attuazione;
3. la natura, l’oggetto, il contesto e le finalità del trattamento e
4. il rischio di varia probabilità e gravità di compressione o violazione dei diritti e delle libertà delle persone fisiche.

Le misure di sicurezza, devono essere adeguate, è imposta quindi un'obbligazione di mezzi (non di risultato), in modo che siano ragionevolmente soddisfacenti alla luce delle conoscenze e delle prassi.

Gli standard internazionali relativi alla sicurezza delle informazioni indicano che la sicurezza dei dati non riguarda solo l'aspetto informatico del trattamento, ma anche l'aspetto organizzativo, a coprire eventi quali la sottrazione o la perdita dei dati e ogni altro evento che possa non renderli disponibili e/o alterarli. Le misure di sicurezza, quindi devono garantire che:

- i dati possano essere consultati, modificati, divulgati o cancellati solo dalle persone autorizzate a farlo (e che tali persone agiscono solo nell'ambito dell'autorità che gli viene concessa);
- i dati trattati siano accurati e completi in relazione alle finalità per cui sono trattati;
- i dati rimangano accessibili e utilizzabili, cioè, in caso di perdita, modifica o distruzione accidentale, si deve essere in grado di recuperarli e prevenire danni alle persone interessate, predisponendo un opportuno piano di continuità operativa.

La predisposizione delle misure di sicurezza richiede che il titolare sia a conoscenza dell'architettura informatica, del luogo e dei supporti con cui sono trattati i dati personali, informazione senza le quali non è possibile definire e implementare misure adeguate.

Le misure di sicurezza si dividono in due categorie: misure organizzative e misure tecniche, che, sempre secondo l'art. 32, comprendono, tra le altre:

- misura tecnica

  a) la pseudonimizzazione e la cifratura dei dati personali;

- requisiti di sicurezza

  b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;

  c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;

  d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Nel caso specifico, nel complesso, le misure tecniche ed organizzative che possono essere ritenute fondamentali sono:

- la crittografia dei dati personali in transito e a riposo;
- l'anonimizzazione (in taluni casi);
- l'utilizzo di autenticazione a due fattori per l'accesso al sistema;
- la definizione di ruoli e responsabilità per il trattamento dei dati personali;
- l'istruzione del personale sulle misure di sicurezza da adottare.

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati personali trattati sono i seguenti:

- Dati di registrazione

  Dati identificativi e di contatto del referente del Titolare che attiva il servizio di digital whistleblowing (RPCT).

- Categorie particolari di dati

  Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

- Dati relativi a condanne penali e reati

  Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

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

Il ciclo di vita del trattamento dei dati in una piattaforma dedicata alla gestione delle segnalazioni di illeciti, come una soluzione di whistleblowing, può essere descritto attraverso le seguenti fasi funzionali:

1. Attivazione della Piattaforma: questa fase iniziale comprende la messa in funzione del sistema e la sua preparazione per l'operatività. Coinvolge l'installazione del software, la verifica delle funzionalità tecniche e l'assunzione di tutte le misure preliminari di sicurezza dei dati.
2. Configurazione della Piattaforma: durante questa fase, la piattaforma viene configurata secondo le esigenze specifiche dell'organizzazione. Questo include l'impostazione dei permessi di accesso, la personalizzazione delle procedure di segnalazione e la definizione dei protocolli di sicurezza e privacy dei dati.
3. Fase d'Uso della Piattaforma: questo stadio rappresenta il periodo operativo effettivo della piattaforma, durante il quale i segnalanti possono caricare le loro segnalazioni e il ricevente preposto (RPCT) può accedervi. Comprende il trattamento attivo dei dati, come la raccolta, l'analisi e la gestione delle segnalazioni, oltre al mantenimento continuo della sicurezza e della protezione dei dati.
4. Fase di Dismissione della Piattaforma: al termine del contratto o alla scadenza degli obblighi legali per le finalità amministrative e contabili, si procede con la dismissione della piattaforma. Questa fase cruciale include la cancellazione sicura di tutti i dati trattati, in conformità con le normative sulla protezione dei dati e le migliori pratiche per prevenire accessi non autorizzati o il recupero dei dati cancellati. Si assicura così che le informazioni personali e sensibili siano definitivamente rimosse dal sistema e da eventuali backup.

Ognuna di queste fasi richiede un'attenzione particolare alle normative vigenti sulla protezione dei dati, come il GDPR nell'Unione Europea, garantendo che il trattamento dei dati personali sia eseguito in maniera legale, corretta e trasparente, nel rispetto dei diritti degli interessati.

Durante la fase d'uso della piattaforma di segnalazione degli illeciti, il ciclo di vita dei dati attraversa diverse tappe cruciali per garantire una gestione efficace, sicura e conforme alle normative dei dati raccolti. Questo ciclo può essere descritto attraverso i seguenti passaggi:

1. Raccolta dei dati: i dati vengono raccolti quando i segnalanti inviano le loro segnalazioni attraverso la piattaforma. Questi dati possono includere informazioni personali, dettagli specifici dell'illecito segnalato, e potenzialmente dati sensibili o categorie particolari di dati personali.

2. Verifica e valutazione: le segnalazioni ricevute sono soggette a una prima verifica per determinare la loro credibilità e rilevanza. Successivamente, viene effettuata una valutazione preliminare per stabilire se la segnalazione richiede un'indagine approfondita.

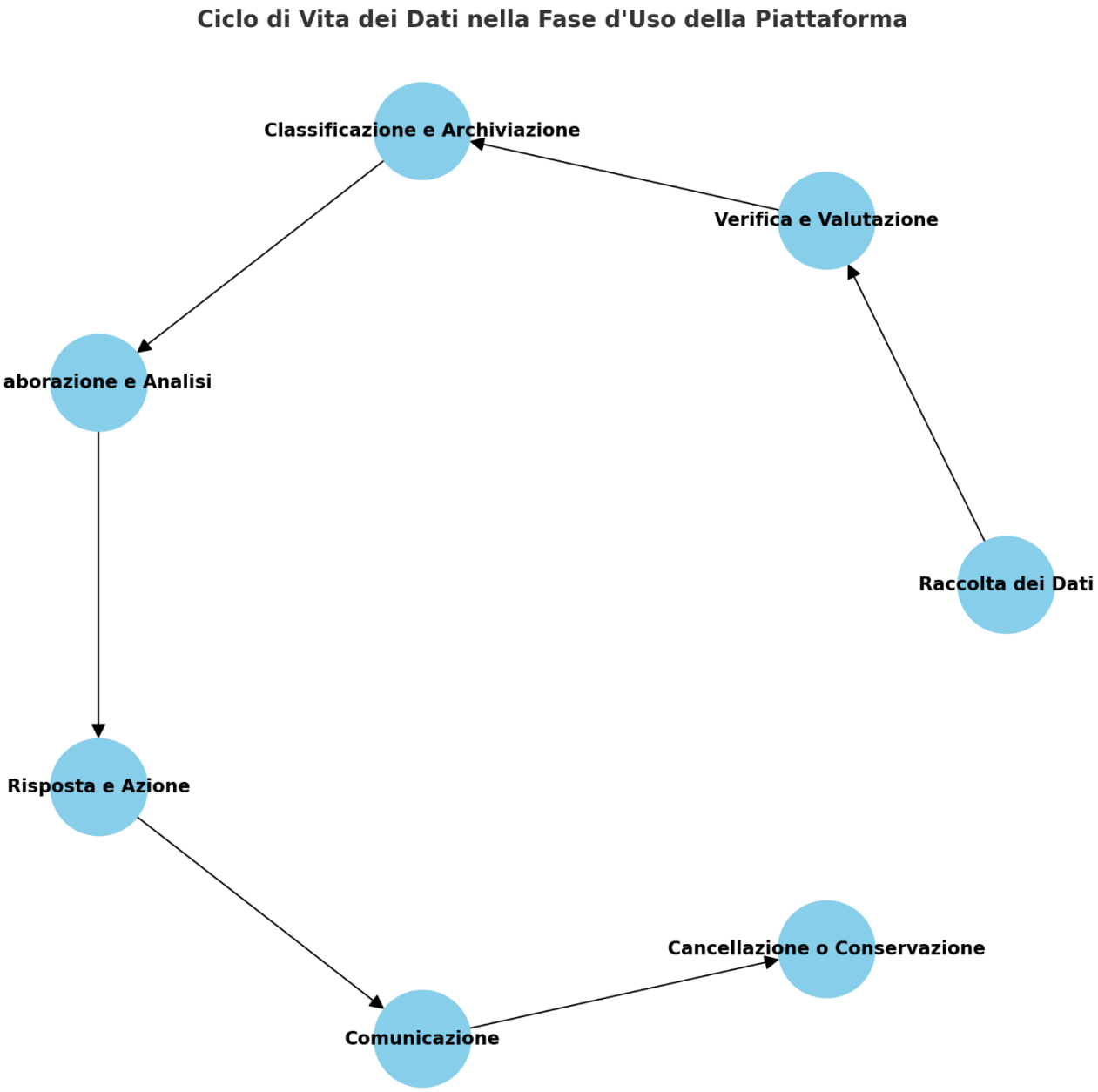
3. Classificazione e archiviazione: i dati raccolti vengono classificati in base alla loro natura e urgenza. Successivamente, sono archiviati in modo sicuro all'interno del sistema, con accesso limitato ai soli utenti autorizzati e in conformità con le politiche di sicurezza dei dati.

4. Elaborazione e analisi: i dati sono analizzati per identificare modelli, rischi potenziali, e per supportare l'indagine sull'illecito segnalato. Questa fase può includere l'aggregazione di dati, l'analisi qualitativa o quantitativa e l'uso di strumenti di intelligence aziendale.

5. Risposta e azione: sulla base dell'analisi, l'organizzazione decide le azioni da intraprendere, che possono includere l'avvio di procedure interne, l'attuazione di misure correttive, o la segnalazione alle autorità competenti.

6. Comunicazione: l'organizzazione può decidere di comunicare l'esito delle indagini ai segnalanti (nel rispetto della loro richiesta di anonimato, se presente) e ad altre parti interessate, secondo le politiche e le procedure stabilite.

7. Cancellazione o conservazione a lungo termine: una volta concluso il processo di gestione della segnalazione, i dati possono essere cancellati in modo sicuro, se non sono più necessari, o conservati per un periodo di tempo definito in conformità con gli obblighi legali e le politiche interne. La conservazione a lungo termine deve garantire la protezione dei dati contro accessi non autorizzati o perdite.



Ogni fase di questo ciclo richiede attenzione costante alle misure di sicurezza dei dati, alla protezione della privacy e al rispetto delle normative applicabili, come il GDPR. L'obiettivo è garantire che i dati personali siano trattati in maniera etica, sicura e legale, preservando i diritti degli individui coinvolti.

Valutazione: Accettabile

Quali sono le risorse di supporto ai dati?

Le risorse che ospitano i dati oggetto del trattamento sono:

- I dispositivi utilizzati dal mittente e dai destinatari;
- le memorie dei server di memorizzazione dei dati;
- gli eventuali i supporti di backup;
- le reti utilizzata per comunicare i dati;

Nello specifico il Software di whistleblowing professionale GlobaLeaks e basato su un’infrastruttura IaaS e SaaS privata basata su tecnologie:

- Linux (Ubuntu Server)
- NGINX
- Python e Node.js
- Google Cloud Virtualization

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Gli scopi del trattamento dei dati personali per i servizi di gestione delle segnalazioni di illeciti sono specifici, espliciti e legittimi.

In particolare, gli scopi del trattamento sono i seguenti:

- inviare segnalazioni di illeciti da parte dei segnalanti agli organismi preposti a gestire tali segnalazioni;
- gestire le segnalazioni, ad esempio registrare l'avvenuta ricezione della segnalazione e gestire le fasi successive;
- garantire la sicurezza e la riservatezza delle segnalazioni.

Questi scopi sono **specifici**, in quanto sono chiaramente definiti e limitati.

Questo principio impedisce l'utilizzo improprio dei dati raccolti, assicurando che siano trattati solo per le finalità di segnalazione degli illeciti, come la prevenzione, l'indagine o la rivelazione di attività illegali, non etiche o dannose all'interno di un'organizzazione.

La specificità degli scopi aiuta a proteggere i diritti dei segnalanti e delle persone coinvolte nelle segnalazioni.

Sono **espliciti**, in quanto sono chiaramente comunicati ai segnalanti e ai destinatari dei dati personali.

Questo assicura trasparenza e consente ai soggetti dei dati di comprendere chiaramente per quali motivi le loro informazioni personali vengono raccolte e trattate.

La trasparenza è fondamentale per costruire fiducia nel sistema di whistleblowing e per incoraggiare le segnalazioni in buona fede.

Sono **legittimi**, in quanto sono conformi alle disposizioni del Regolamento generale sulla protezione dei dati (GDPR) e alle normative di settore.

Il trattamento dei dati per scopi di whistleblowing si basa sulla necessità di rilevare e gestire le violazioni legali, etiche o regolamentari e di promuovere un ambiente di lavoro sicuro, etico e conforme alle leggi.

Nel caso specifico, D.Lgs. 24/2023 in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali rappresenta la base giuridica a fondamento delle liceità del trattamento.

In conclusione, definire scopi di trattamento specifici, espliciti e legittimi nel contesto del whistleblowing è essenziale per garantire che il sistema sia utilizzato in modo responsabile, etico e conforme alle leggi sulla protezione dei dati. Ciò contribuisce a proteggere le persone coinvolte, a

promuovere la trasparenza e l'integrità organizzativa e a rafforzare la fiducia nell'uso dei sistemi di segnalazione degli illeciti.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Le basi legali per il trattamento dei dati personali sono fondamentali per garantire che tale trattamento sia conforme alla legge. Nel contesto del Regolamento Generale sulla Protezione dei Dati (GDPR) dell'Unione Europea, che è uno dei principali quadri normativi in materia, sono previste diverse basi legali che rendono lecito il trattamento dei dati personali. Queste basi legali possono essere applicate anche nel contesto di un sistema di whistleblowing, a seconda delle circostanze specifiche e degli obiettivi perseguiti. Le principali includono:

1. Consenso: il soggetto dei dati ha dato il proprio consenso esplicito al trattamento dei propri dati personali per una o più finalità specifiche. Nel contesto del whistleblowing, il consenso potrebbe essere applicabile in certe situazioni, ma spesso non è la base legale primaria, dato il contesto e la natura delle segnalazioni.
2. Obblighi legali: il trattamento è necessario per adempiere a un obbligo legale al quale il titolare del trattamento è soggetto. Questa base legale è spesso rilevante per il whistleblowing, in quanto le organizzazioni possono avere l'obbligo legale di gestire e indagare sulle segnalazioni di illeciti.
3. Protezione degli interessi vitali: il trattamento è necessario per proteggere gli interessi vitali del soggetto dei dati o di un'altra persona fisica. Questa base legale potrebbe essere applicata in situazioni estreme, dove le segnalazioni di illeciti riguardano minacce immediate alla sicurezza o alla vita delle persone.
4. Esecuzione di un compito di interesse pubblico o nell'esercizio di pubblici poteri: il trattamento è necessario per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri conferiti al titolare del trattamento. Questo può essere applicabile a enti pubblici o organizzazioni che svolgono funzioni di interesse pubblico.
5. Interessi legittimi: il trattamento è necessario per il perseguimento degli interessi legittimi perseguiti dal titolare del trattamento o da terzi, a meno che non prevalgano gli interessi o i diritti e le libertà fondamentali del soggetto dei dati che richiedono la protezione dei dati personali. Le organizzazioni possono basare il trattamento su questa base legale per il trattamento dei dati nel contesto del whistleblowing, purché tale trattamento non pregiudichi indebitamente i diritti dei soggetti dei dati.

La base giuridica prevalente per il trattamento dei dati personali nell'ambito dei sistemi di whistleblowing si fonda principalmente sull'esecuzione di compiti di interesse pubblico, così come definito dagli articoli 6, paragrafo 1, lettera c), 9, paragrafo 2, lettera b), e articolo 10 del Regolamento Generale sulla Protezione dei Dati (GDPR). Questa base si manifesta nell'adempimento di obblighi legali a cui è soggetto il titolare del trattamento, in conformità con quanto stabilito dal Decreto Legislativo 24/2023.

In particolare:

- l'articolo 6, paragrafo 1, lettera c) del GDPR stabilisce che il trattamento è lecito se necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento e ciò implica che, quando esiste un obbligo legale specifico che richiede il trattamento dei dati personali, tale trattamento diventa necessario e legittimo;

- l'articolo 9, paragrafo 2, lettera b) del GDPR prevede eccezioni alla proibizione di trattare categorie particolari di dati personali (come quelli che rivelano origini razziali o etniche, opinioni politiche, convinzioni religiose o filosofiche, o l'appartenenza sindacale), consentendone il trattamento se necessario per adempiere obblighi e esercitare specifici diritti del titolare del trattamento o dell'interessato nel campo del lavoro e della sicurezza sociale e della protezione sociale;
- l'articolo 10 del GDPR si riferisce al trattamento di dati personali relativi a condanne penali e reati o a misure di sicurezza connesse, stabilendo che tale trattamento deve essere regolato dalla legge dell'Unione o degli Stati membri.

Il D.Lgs. 24/2023, integrando il GDPR, fornisce il quadro normativo specifico per il trattamento dei dati nel contesto del whistleblowing, definendo gli obblighi legali e le condizioni sotto le quali tali dati possono essere trattati. Ciò assicura che il trattamento dei dati personali, comprese le segnalazioni di illeciti, sia condotto in maniera conforme ai principi di legalità, trasparenza e protezione dei diritti degli interessati.

I D.Lgs. 24/2024 e 231/2001 contemplano l'utilizzo dei dati anagrafici qualora la segnalazione effettuata sia circonstanziata e ritenuta valida da parte di chi ha effettuato l'istruttoria, parallelamente, regolamentino tutte le tutele che devono essere garantite nei confronti del whistleblower dopo aver effettuato una segnalazione (i.e. mobbing, allontanamento, demansionamento, riduzioni di orario etc.).

Valutazione: Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

In generale, i dati raccolti per i servizi di notifiche digitali sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati.

Per quanto riguarda la fase di attivazione della piattaforma

Per attivare il servizio, si richiedono esclusivamente i dati personali dell'utente che registra l'accesso (nome, cognome, ruolo, numero di telefono, e-mail professionale) e informazioni sull'ente di appartenenza (nome, indirizzo, codice fiscale e partita IVA).

Per quanto riguarda la fase d'uso della piattaforma

Il software dedicato al whistleblowing elabora le segnalazioni utilizzando questionari avanzati, sviluppati in collaborazione con prestigiosi istituti di ricerca specializzati in whistleblowing e anticorruzione, e conformemente alle direttive di Transparency International Italia, basandosi sulla normativa attuale.

Adottando il principio di "privacy by design", tutti gli strumenti impiegati, come il software GlobaLeaks, i log di sistema e i firewall, sono impostati per escludere la registrazione di qualsiasi dato che potrebbe compromettere la privacy o l'anonimato del segnalante, quali indirizzi IP, User Agents e altri metadati.

L'applicazione GlobaLeaks supporta l'uso del Tor Browser, permettendo un accesso anonimo che rispecchia le più recenti innovazioni tecnologiche in materia di protezione dell'identità online.

La raccolta dati si limita a quanto strettamente necessario per autenticare l'identità del whistleblower, garantendo che le segnalazioni siano fondate e responsabilizzando l'individuo rispetto alle informazioni condivise.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

Nel caso servizio di segnalazione degli illeciti, la garanzia che i dati siano esatti e aggiornati è particolarmente importante, in quanto tali dati possono avere un impatto significativo sulla vita del destinatario.

Nel caso servizio di segnalazione degli illeciti il titolare del trattamento deve adottare misure organizzative per garantire l'esattezza e l'aggiornamento dei dati:

- Verifica dei dati al momento della raccolta: al momento della raccolta dei dati, il titolare del trattamento deve verificare che i dati siano corretti e completi;
- Protezione dei dati: il titolare del trattamento deve adottare misure per proteggere i dati da accessi non autorizzati o alterazioni, come per esempio protocolli di sicurezza per proteggere la trasmissione e la conservazione dei dati.

Adottando queste misure, il titolare del trattamento può contribuire a garantire che i dati raccolti per i servizi di notifiche digitali siano esatti e aggiornati, in conformità al GDPR.

Comunque, l'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.

Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

I dati raccolti verranno conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati. I dati verranno quindi conservati, ex lege dall'articolo 14 del Decreto legislativo n. 24, per un periodo di 5 anni dalla data di comunicazione dell'esito finale della procedura di segnalazione e comunque per tutta la durata dell'eventuale procedimento disciplinare, penale o dinanzi la Corte dei conti

Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

L'interessato deve essere informato del trattamento dei suoi dati personali in modo trasparente e comprensibile.

L'informativa deve essere fornita al momento della raccolta dei dati o, se i dati sono raccolti da altre fonti, entro un mese dalla raccolta.

L'informativa deve includere le seguenti informazioni:

- l'identità e i dati di contatto del titolare del trattamento;
- le finalità del trattamento;

- le categorie di dati personali trattati;
- i destinatari o le categorie di destinatari a cui i dati personali possono essere comunicati;
- il periodo di conservazione dei dati personali;
- i diritti dell'interessato, in particolare il diritto di accesso, di rettifica, di cancellazione, di limitazione del trattamento, di portabilità dei dati, di opposizione al trattamento e di reclamo all'autorità di controllo.

Nel caso del servizio di gestione delle segnalazioni l'informativa è fornita:

- al termine della compilazione del questionario che si conclude con una schermata che indicato dove è reperibile l'informativa privacy completa;
- tramite un link presente sul sito web del titolare del trattamento.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso dell'interessato è richiesto in specifiche circostanze delineate dal D.Lgs. 24/2023. Tale consenso diventa necessario solo quando si debba rivelare l'identità del segnalante a individui al di fuori del gruppo autorizzato a ricevere o gestire le segnalazioni, come specificato nel comma 2 dell'articolo 12, o nel contesto di un procedimento giudiziario. In quest'ultimo caso, la richiesta di consenso si rende indispensabile qualora l'accusa si basi, interamente o parzialmente, sulla segnalazione e l'identificazione del segnalante sia essenziale per consentire la difesa dell'accusato, come indicato nel comma 5 dello stesso articolo.

Per ottenere il consenso degli interessati in queste situazioni, è fondamentale adottare un approccio chiaro e trasparente. L'interessato deve essere informato in maniera dettagliata sui motivi specifici per cui si richiede la divulgazione della sua identità, sui potenziali destinatari di tale informazione e sulle conseguenze della sua decisione di concedere o negare il consenso. Questo processo deve garantire che l'interessato abbia a disposizione tutte le informazioni necessarie per prendere una decisione consapevole e che il suo consenso sia espresso liberamente, specifico per quella situazione e inequivocabile.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di accesso?

Nel contesto del whistleblowing, il diritto di accesso consente agli interessati di richiedere e ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento dei dati personali che li riguardano e, in caso affermativo, di accedere a tali dati. Questo diritto è garantito dall'**articolo 15 del Regolamento UE 2016/679**. Ecco come gli interessati possono esercitarlo:

1. Presentazione della richiesta: l'interessato deve inviare una richiesta formale al titolare del trattamento dei dati. Questa richiesta può solitamente essere fatta per iscritto, via e-mail o tramite qualsiasi altro mezzo previsto dall'organizzazione che gestisce il sistema di whistleblowing. È importante che la richiesta specifichi chiaramente che si tratta di un'esercitazione del diritto di accesso secondo il GDPR.
2. Identificazione: l'organizzazione può richiedere la verifica dell'identità dell'interessato per prevenire l'accesso non autorizzato ai dati personali. Questo passaggio è fondamentale per proteggere la privacy e la sicurezza dei dati.

3. Risposta del titolare del trattamento: il titolare del trattamento deve fornire una risposta alla richiesta senza ingiustificato ritardo e in ogni caso entro un mese dal ricevimento della richiesta. La risposta dovrebbe includere tutte le informazioni richieste, come la conferma dell'esistenza del trattamento dei dati personali, le finalità del trattamento, le categorie di dati personali in questione, e i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati.

4. Accesso ai dati: se in corso il trattamento dei dati personali dell'interessato, il titolare del trattamento deve fornire una copia dei dati oggetto di trattamento. Per le copie successive richieste dall'interessato, l'organizzazione può addebitare un costo ragionevole basato sui costi amministrativi.

5. Informazioni aggiuntive: la risposta dovrebbe anche includere informazioni sui diritti dell'interessato di rettificare o cancellare i dati personali, limitare il trattamento, opporsi al trattamento, e il diritto di presentare un reclamo a un'autorità di controllo.

6. Ricorso: se l'interessato non è soddisfatto della risposta ricevuta o se la richiesta viene negata senza una motivazione valida, ha il diritto di presentare un reclamo all'autorità di protezione dei dati competente.

Le organizzazioni dovrebbero avere procedure chiare e facilmente accessibili per permettere agli interessati di esercitare i loro diritti, compreso il diritto di accesso. È fondamentale che queste procedure siano progettate tenendo conto della necessità di proteggere l'anonimato dei segnalanti e la confidenzialità delle informazioni nel contesto del whistleblowing.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto alla portabilità dei dati?

Nel contesto del whistleblowing, l'esercizio del diritto alla portabilità dei dati da parte degli interessati, come definito dall'**articolo 20 del Regolamento UE 2016/679**, può presentare delle particolarità. Il diritto alla portabilità consente agli individui di ricevere i dati personali che li riguardano, forniti a un titolare del trattamento, in un formato strutturato, di uso comune e leggibile da dispositivo automatico, e di trasmettere tali dati a un altro titolare del trattamento senza impedimenti.

Tuttavia, nel caso specifico del whistleblowing, alcuni fattori possono limitare l'applicabilità di questo diritto:

1. Natura dei dati: il diritto alla portabilità si applica ai dati personali che un interessato ha fornito attivamente e consapevolmente o tramite l'uso di un servizio. Le segnalazioni di whistleblowing spesso contengono informazioni che vanno oltre i dati personali forniti volontariamente dall'interessato, includendo valutazioni, giudizi, o altre informazioni elaborate nel corso dell'istruttoria.

2. Base giuridica: il diritto alla portabilità dei dati si applica principalmente nei casi in cui il trattamento si basa sul consenso dell'interessato (articolo 6(1)(a)) o su un contratto (articolo 6(1)(b)). Nel whistleblowing, il trattamento dei dati è spesso giustificato dall'esecuzione di un compito di interesse pubblico o dall'adempimento di un obbligo legale (articolo 6(1)(c)), situazioni in cui il diritto alla portabilità può non essere direttamente applicabile.

3. Confidenzialità e protezione degli Interessati: considerando la natura sensibile delle segnalazioni di whistleblowing e la necessità di proteggere sia i segnalanti che le persone segnalate, l'applicazione del diritto alla portabilità dei dati deve essere valutata attentamente per non compromettere misure di riservatezza e anonimato.

Pertanto, sebbene il GDPR preveda il diritto alla portabilità dei dati, nel contesto del whistleblowing la sua applicazione deve essere analizzata caso per caso, valutando la base giuridica del trattamento, la natura dei dati trattati, e la necessità di bilanciare tale diritto con la protezione degli interessi coinvolti. In molte situazioni specifiche di whistleblowing, questo diritto potrebbe non essere esercitabile nello stesso modo in cui lo sarebbe per altri tipi di trattamento dati.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di rettifica?

Nel contesto del whistleblowing, il diritto di rettifica, garantito dall'**articolo 16 del Regolamento UE 2016/679**, consente agli interessati di ottenere dal titolare del trattamento la correzione di dati inesatti che li riguardano senza ingiustificato ritardo. Questo diritto è fondamentale per assicurare l'accuratezza delle informazioni trattate e proteggere l'integrità dei dati personali.

Per esercitare il diritto di rettifica nel caso specifico del whistleblowing, gli interessati possono seguire questi passi:

1. Identificazione del titolare del trattamento: l'interessato deve identificare chi è il titolare del trattamento dei dati all'interno dell'organizzazione che gestisce il sistema di whistleblowing. Questa informazione è solitamente disponibile nella politica sulla privacy o nel documento informativo fornito al momento della raccolta dei dati.
2. richiesta formale: l'interessato dovrebbe inviare una richiesta formale di rettifica al titolare del trattamento. La richiesta può essere redatta in forma scritta o elettronica, specificando quali dati si ritengono inaccurati o incompleti e fornendo le correzioni o gli aggiornamenti necessari.
3. Fornire prove: se possibile, l'interessato dovrebbe allegare alla richiesta qualsiasi documento o prova che supporti la necessità di rettifica dei dati.
4. Tempistiche di risposta: il titolare del trattamento deve agire sulla richiesta di rettifica senza ingiustificato ritardo e, in ogni caso, entro un mese dalla ricezione della richiesta. Questo termine può essere prorogato di due mesi in casi di particolare complessità, ma il titolare del trattamento deve informare l'interessato del ritardo e dei motivi dello stesso entro un mese dalla ricezione della richiesta.
5. notifica delle modifiche: una volta effettuate le rettifiche, il titolare del trattamento dovrebbe notificare all'interessato che le modifiche sono state apportate. Se i dati inesatti sono stati condivisi con terze parti, il titolare del trattamento dovrebbe anche informare queste parti delle correzioni effettuate, a meno che ciò non si riveli impossibile o comporti uno sforzo sproporzionato.
6. ricorso: se la richiesta di rettifica viene negata o non adeguatamente soddisfatta, l'interessato ha il diritto di presentare un reclamo all'autorità di controllo competente o di adire le vie legali.

È importante che le organizzazioni che implementano sistemi di whistleblowing stabiliscano procedure chiare e accessibili per consentire agli interessati di esercitare i loro diritti, inclusi quelli di rettifica, assicurando al contempo la protezione dei segnalanti e il rispetto delle normative sulla privacy.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di cancellazione (diritto all'oblio)?

Nel contesto del whistleblowing, il diritto alla cancellazione, noto anche come diritto all'oblio, consente agli interessati di richiedere la rimozione dei loro dati personali dal sistema di trattamento del titolare, in determinate circostanze. Questo diritto è garantito dall'**articolo 17 del Regolamento 2016/679**. Di seguito viene illustrato come gli interessati possono esercitarlo:

1. Invio della richiesta: l'interessato deve presentare una richiesta formale di cancellazione dei propri dati personali al titolare del trattamento. La richiesta può essere inviata tramite i canali comunicativi previsti dall'organizzazione, quali e-mail, piattaforme online dedicate o attraverso moduli specifici.
2. Verifica dell'identità: al fine di prevenire eliminazioni errate o fraudolente, il titolare del trattamento può richiedere all'interessato di fornire una prova della propria identità. Questo passo è cruciale per assicurare che la richiesta di cancellazione provenga effettivamente dall'interessato cui si riferiscono i dati.
3. Valutazione della richiesta: il titolare del trattamento deve valutare la richiesta di cancellazione tenendo conto delle basi legali per il trattamento dei dati e delle eccezioni previste dal GDPR. In particolare, il diritto alla cancellazione non è assoluto e può essere limitato da necessità quali l'adempimento di obblighi legali o l'esercizio del diritto alla libertà di espressione e informazione.
4. Risposta dell'organizzazione: il titolare del trattamento è tenuto a rispondere senza ingiustificato ritardo, solitamente entro un mese dalla ricezione della richiesta. Se la richiesta di cancellazione viene accettata, il titolare deve procedere con la rimozione dei dati personali e, ove possibile, notificare la cancellazione a eventuali terze parti che hanno ricevuto i dati.
5. Comunicazione ai terzi: se i dati personali sono stati divulgati a terzi, il titolare del trattamento deve informare tali terzi della richiesta di cancellazione, a meno che ciò non si riveli impossibile o comporti uno sforzo sproporzionato.
6. Ricorso: qualora l'interessato non sia soddisfatto della gestione della sua richiesta da parte del titolare del trattamento o se la richiesta viene negata, ha il diritto di presentare un reclamo presso l'autorità di controllo competente e/o adire le vie legali.

È importante notare che, nel contesto del whistleblowing, il diritto alla cancellazione deve essere bilanciato con altri interessi legittimi, come la necessità di condurre indagini sugli illeciti segnalati o di conservare i dati per motivi di accountability e conformità legale. Pertanto, l'applicabilità del diritto alla cancellazione può variare a seconda delle circostanze specifiche del trattamento e delle normative applicabili.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di limitazione?

Nel contesto del whistleblowing, il diritto di limitazione del trattamento consente agli interessati di richiedere la sospensione del trattamento dei propri dati personali in determinate circostanze. Questo diritto è previsto dall'**articolo 18 del Regolamento 2016/679**. Di seguito viene illustrato come gli interessati possono esercitarlo:

1. Presentazione della richiesta: l'interessato deve inoltrare una richiesta formale al titolare del trattamento, specificando che si intende esercitare il diritto di limitazione secondo il GDPR. La richiesta può essere fatta attraverso i canali predisposti dall'organizzazione, come e-mail, piattaforme online, o moduli dedicati.
2. Condizioni per la limitazione: l'interessato deve indicare le specifiche circostanze che giustificano la limitazione del trattamento, come previsto dall'articolo 18 del GDPR. Queste includono situazioni in cui:
   - l'accuratezza dei dati personali è contestata dall'interessato, per il periodo necessario al titolare del trattamento per verificare l'accuratezza di tali dati;
   - il trattamento è illecito, e l'interessato si oppone alla cancellazione dei dati personali, richiedendo invece la limitazione del loro uso;
   - il titolare del trattamento non ha più bisogno dei dati personali ai fini del trattamento, ma sono richiesti dall'interessato per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria;
   - l'interessato si è opposto al trattamento in attesa della verifica relativa all'eventuale prevalenza dei motivi legittimi del titolare del trattamento rispetto a quelli dell'interessato.
3. Valutazione e risposta: il titolare del trattamento deve valutare la richiesta e rispondere senza ingiustificato ritardo, di norma entro un mese. Se accetta la richiesta di limitazione, il trattamento dei dati personali dell'interessato sarà limitato al solo immagazzinamento, a meno che non si dia il consenso dell'interessato a ulteriori trattamenti o per la tutela di diritti legali o per proteggere i diritti di un'altra persona fisica o giuridica.
4. Notifica di limitazione: qualora il titolare del trattamento abbia limitato il trattamento di dati personali, deve informare l'interessato prima di revocare tale limitazione.
5. Ricorso: se l'interessato non è soddisfatto della decisione del titolare del trattamento o se la richiesta di limitazione viene negata, ha il diritto di presentare un reclamo all'autorità di controllo e/o adire le vie legali.

L'implementazione di procedure chiare per l'esercizio del diritto di limitazione del trattamento è fondamentale nelle organizzazioni che gestiscono segnalazioni di whistleblowing, al fine di garantire il rispetto dei diritti degli interessati, pur mantenendo l'integrità delle indagini sugli illeciti segnalati.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritto di opposizione?

Nel contesto del whistleblowing, il diritto di opposizione consente agli interessati di opporsi al trattamento dei loro dati personali quando questo è basato su determinate basi legali, comprese quelle relative all'esecuzione di un compito di interesse pubblico o all'esercizio di pubblici poteri. Questo diritto è previsto dall'**articolo 21 del Regolamento UE 2016/679**. Di seguito viene illustrato come gli interessati possono esercitarlo:

1. Invio della richiesta: l'interessato deve formulare una richiesta formale di opposizione al titolare del trattamento, specificando che desidera esercitare il proprio diritto di opposizione secondo quanto stabilito dall'articolo 21 del GDPR. La richiesta può essere inviata tramite i mezzi predisposti dall'organizzazione, come e-mail, form online o altri canali di comunicazione.
2. Motivazione della richiesta: è importante che l'interessato fornisca una motivazione specifica per la sua opposizione al trattamento dei dati personali. Nel contesto del whistleblowing, l'opposizione potrebbe essere basata sulla particolare situazione dell'interessato che giustifica la richiesta di interrompere il trattamento.
3. Valutazione da parte del titolare del trattamento: una volta ricevuta la richiesta, il titolare del trattamento deve valutare se i motivi dell'interessato prevalgono sui legittimi motivi del titolare per proseguire il trattamento. Se il trattamento dei dati era diretto al marketing, l'opposizione deve essere accolta senza eccezioni.
4. Risposta all'interessato: Il titolare del trattamento deve comunicare all'interessato la propria decisione senza ingiustificato ritardo, generalmente entro un mese dalla ricezione della richiesta. Se il titolare del trattamento decide di accogliere l'opposizione, il trattamento dei dati personali in questione dovrà cessare immediatamente.
5. Ricorso: qualora l'interessato non sia soddisfatto della risposta o se la sua richiesta viene negata, ha il diritto di presentare un reclamo all'autorità di protezione dati competente e/o di adire le vie legali.

Nel contesto specifico del whistleblowing, l'esercizio del diritto di opposizione può presentare delle problematiche, soprattutto quando il trattamento dei dati è necessario per adempiere a obblighi legali, per l'esecuzione di compiti di interesse pubblico o per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria. Tuttavia, le organizzazioni devono garantire che i diritti degli interessati siano rispettati e che esistano procedure chiare e accessibili per la loro esercitazione.

Il diritto è in ogni caso esercitabile nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196.

Valutazione: Accettabile

Come fanno gli interessati a esercitare i loro diritti?

PROCEDURA PER L'ESERCIZIO DEI DIRITTI

Il Titolare assicura agli interessati l'esercizio dei propri diritti, in particolare quelli

- di accesso ai dati personali conservati presso il Titolare;
- di opporsi al trattamento dei dati;
- di chiedere una copia dei dati;
- di chiedere la cancellazione dei dati;

- di ottenere il blocco dei dati trattati in violazione di legge.

Come già riportato, gli interessati possono esercitare in rari casi il diritto di aggiornamento, rettificazione in considerazione della natura del trattamento.

La risposta ad una richiesta di accesso può comprendere eventuali dati riferiti a terzi nei soli casi in cui la scomposizione dei dati trattati o la privazione di alcuni elementi renda incomprensibili i dati personali relativi all'interessato ed ove non siano lesi i diritti e le libertà altrui.

Gli interessati possono trasmettere le proprie richieste mediante la compilazione di un modulo predisposto dal Titolare e messo a disposizione sul sito internet istituzionale, da inviarsi via e-mail all'indirizzo indicato nel modulo.

Il Titolare fornisce all'interessato le informazioni richieste senza ingiustificato ritardo e, comunque, al più tardi entro un mese dal ricevimento della richiesta stessa. Se necessario, tale termine può essere prorogato di due mesi ove la richiesta sia trasmessa senza l 'utilizzo del modulo sopra indicato e ciò abbia reso necessari tempi lunghi di lavorazione della domanda o in conseguenza della complessità o del numero delle richieste. Il Titolare informa l'interessato di tale proroga, e dei motivi del ritardo, entro un mese dal ricevimento della richiesta.

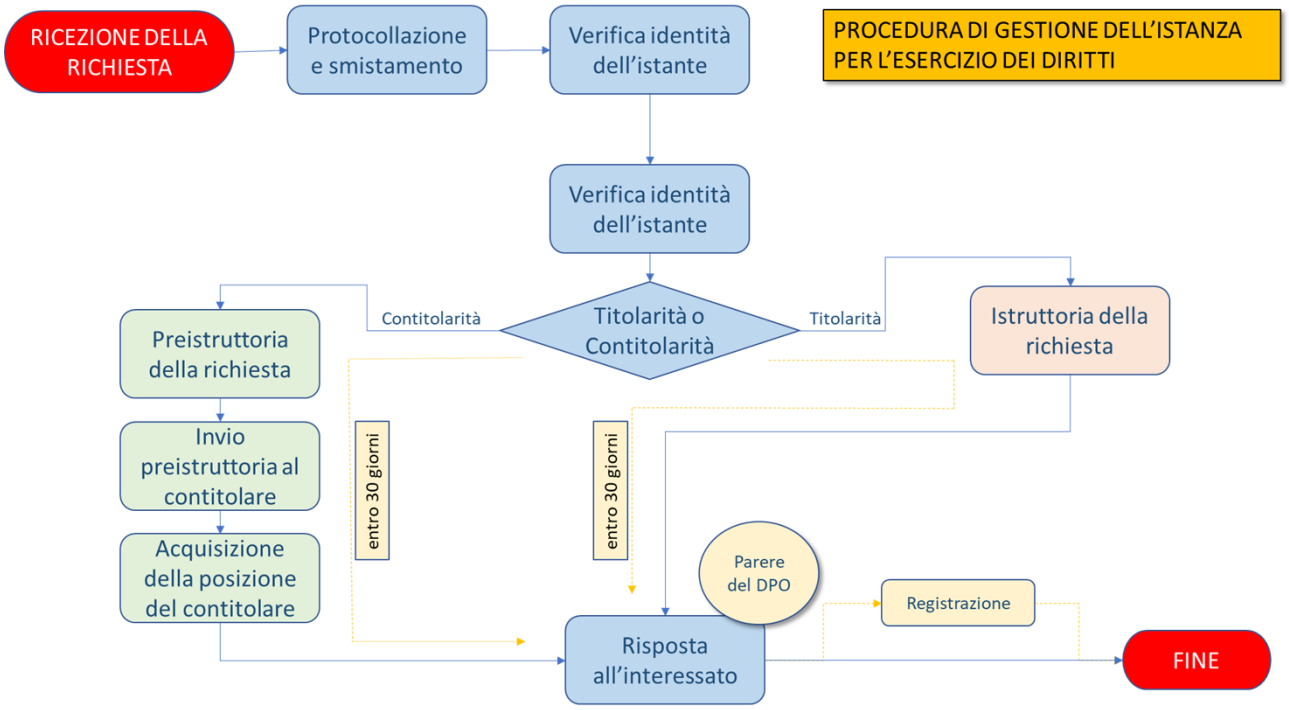
Ove il Titolare di trattamento, non fosse in grado di identificare i dati personali oggetto della richiesta dell'interessato o non avesse certezza del fatto che i dati oggetto della richiesta sono propri dell'interessato, ne informa l'interessato, chiedendo di fornire ulteriori informazioni. In tali casi, il termine per la risposta decorre dal momento della risposta dell'interessato alla richiesta di integrazione.

L'interessato ha il diritto di presentare reclamo al Data Protection Officer designato e/o al Garante per la Tutela dei dati personali.

TABELLA SINTESI ESERCIZIO DIRITTI CONCRETAMENTE ESERCITABILI	
Diritto	**Regolamento UE 2016/679**
Diritto di accesso	Esercitabile
Diritto alla portabilità	Solo in alcuni specifici casi
Diritto di rettifica	Esercitabile
Diritti di cancellazione (oblio)	Esercitabile
Diritto di limitazione	Esercitabile
Diritto di opposizione	Esercitabile

FASI DEL PROCESSO DI GESTIONE DELLA RICHIESA DI ESERCIZIO DEI DIRITTI

Il flusso di gestione di una richiesta di esercizio dei diritti è di seguito rappresentato:



Valutazione: Accettabile

<u>Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?</u>

Nel caso si riveli necessario fare ricorso ad un responsabile esterno del trattamento, gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati con atto di nomina (contratto) ai sensi e per gli effetti del art. 28 Reg. UE 2016/679.

Ogni contratto definisce la tipologia del trattamento e dati trattati e con riferimento agli obblighi inerenti al mandato del Responsabile lo impegna ad adottare tutte le misure necessarie all'attuazione delle disposizioni di legge contenute nel Reg.to Europeo 2016/679. Il contratto definisce dello specifico:

- i termini relativi al trattamento dei dati;

- le modalità di comunicazione di dati;

- le misure per garantire l'affidabilità del trattamento e la non divulgazione dei dati;

- le misure tecniche ed organizzative adeguate a garantire la sicurezza del trattamento;

- la catena delle responsabilità;

- i diritti degli interessati;

- le modalità di gestione delle eventuali violazione dei dati personali;

- la collaborazione richiesta per l'effettuazione della valutazione d'impatto sulla protezione dei dati personali;

- le modalità operative per la cancellazione o la restituzione dei dati;

- il diritto di audit del titolare nei confronti del responsabile;

- le modalità per un eventuale trasferimento di dati personali da parte del Responsabile nei confronti di un sub-responsabile;

- l'impegno all'adozione e rispetto di codici di condotta e certificazioni;

- una serie di condizioni generali.

Gli accordi contrattuali sono definiti:

- tra l'ENTE e ASMEL rispettivamente in qualità di Titolare e di Responsabile del trattamento
- tra ASMEL e ASMENET rispettivamente in qualità di Responsabile e Sub-Responsabile del trattamento

Valutazione: Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea.

Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

	Misura	Situazione in essere	Azione di miglioramento
1	**Procedure per l'utilizzo delle notifiche digitali**	**Adeguata**	**Nessuna**
		Sono presenti procedure operative per la gestione delle notifiche digitali	
2	**Registro dei trattamenti**	**Adeguata**	**Nessuna**
		Il trattamento è stato inserito nel registro dei trattamenti.	
3	**Informativa**	**Adeguata**	**Nessuna**
		È presente un'informativa ed è pubblicata sul sito dell'ente	
4	**Esercizio dei diritti degli interessati**	**Adeguata**	**Nessuna**
		È stata definita, approvata e pubblicata una procedura per la gestione dell'esercizio dei diritti degli interessati	
5	**Tracciabilità**	**Adeguata**	**Nessuna**
		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. Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse. 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.	
6	**Archiviazione**	**Adeguata**	**Nessuna**
		L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.	
7	**Minimizzazione dei dati**	**Adeguata**	**Nessuna**
		Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, E-mail di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia.	

	Misura	Situazione in essere	Azione di miglioramento
8	**Manutenzione**	**Adeguata**	**Nessuna**
		È prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Asmenet attraverso cui svolgere le modifiche al sistema installare 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 del Sub-Responsabile e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.	
9	**Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento)**	**Adeguata**	**Nessuna**
		Gli accordi contrattuali sono definiti: • tra l'ENTE e ASMEL rispettivamente in qualità di Titolare e di Responsabile del trattamento • tra ASMEL e ASMENET rispettivamente in qualità di Responsabile e Sub-Responsabile del trattamento	
10	**Anonimizzazione**	**Adeguata**	**Nessuna**
		L'anonimato degli utenti è protetto mediante la tecnologia Tor. L'intera applicazione ritiene di evitare la registrazione di metadati sensibili che potrebbero portare all'identificazione degli informatori.	
11	**Politica di tutela della privacy**	**Adeguata**	**Nessuna**
		L'ufficio ha implementato un'organizzazione interna pienamente idonea a garantire l'adeguatezza della protezione dei dati personali sono state adeguatamente formalizzate le nomine e le istruzioni dei i soggetti interni autorizzati ad effettuare il trattamento dei dati personali.	
12	**Formazione continua**	**Adeguata**	**Nessuna**
		Il Comune ha implementato un programma di formazione continua per i soggetti autorizzati al trattamento dei dati personali.	
13	**Gestire gli incidenti di sicurezza e le violazioni dei dati personali**	**Adeguata**	**Nessuna**
		Il Sub-Responsabile ha definito una procedura per la gestione delle violazioni dei dati personali.	
14	**Vigilanza sulla protezione dei dati**	**Adeguata**	**Nessuna**
		Il DPO/RPD ha effettuato un audit iniziale finalizzato a verificare che siano state correttamente attuate le misure tecniche ed organizzative per garantire adeguata protezione dei dati personali e sono programmati audit periodici.	
15	**Lotta contro il malware**	**Adeguata**	**Nessuna**
		Tutti i computer del personale del Sub-Responsabile 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. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla	

	Misura	Situazione in essere	Azione di miglioramento
		tematica tramite formazione diretta o documentazione online.	
16	**Certificazioni sulla sicurezza delle informazioni**	**Adeguata**	**Nessuna**
		Il Sub-Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato: • ISO/IEC 27001:2017 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO 9001:2015 • ISO 37001:2016 • ACN	
17	**Prevenzione delle fonti di rischio**	**Adeguata**	**Nessuna**
		È stata effettuata una valutazione dei rischi che ha preso in considerazione tutti i possibili accadimenti valutandone l'adeguatezza delle misure di mitigazione dei rischi messe in atto	
18	**Gestione dei rischi**	**Adeguata**	
		La piattaforma utilizzata offre un buon grado di business continuity in particolare i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.	
19	**Crittografia**	**Adeguata**	**Nessuna**
		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 Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto	
20	**Controllo degli accessi logici**	**Adeguata**	**Nessuna**
		L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.	

	Misura	Situazione in essere	Azione di miglioramento
21	**Gestione postazioni**	**Adeguata**	**Nessuna**
		Le postazioni o altri dispositivi, che consentono di accedere alle immagini, sono dotati di adeguati controlli logici di accesso per garantire che le persone che li utilizzano siano solo quelle autorizzate formalmente a effettuare i trattamenti.	
22	**Sicurezza dei canali informatici**	**Adeguata**	**Nessuna**
		Tutte le connessioni sono protette tramite protocollo TLS 1.2= Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.	
23	**Sicurezza dell'hardware**	**Adeguata**	**Nessuna**
		I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7:24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7:24. I datacenter del fornitore IaaS sono certificati ISO27001	
24	**Sicurezza dell'applicazione web**	**Adeguata**	**Nessuna**
		Applicazioni Web implementata in aderenza alle Linee Guida di Sicurezza OWASP	
25	**Gestione delle vulnerabilità tecniche**	**Adeguata**	**Nessuna**
		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 crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente.	
26	**Backup**	**Adeguata**	**Nessuna**
		I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.	

Valutazione del sistema per la gestione delle segnalazioni di illeciti

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Comunicazione dei dati non autorizzata, diffusione dei dati non autorizzata

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Malware, hacker, cancellazione involontaria, furto del dispositivo.

Quali sono le fonti di rischio?
Fonte umana esterna, fonte umana interna

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?
Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Informativa, Esercizio dei diritti degli interessati, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Crittografia, Controllo degli accessi logici, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Sicurezza dell'applicazione web, Vulnerabilità,

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?
Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Esercizio dei diritti degli interessati, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Crittografia, Controllo degli accessi logici, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Sicurezza dell'applicazione web, Vulnerabilità,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?
Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:
Limitato (Medio)

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce e alle fonti di rischio?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:
Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?
Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:
Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:
Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Accesso illegittimo ai dati)?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e

in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Improbabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Accesso illegittimo ai dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Trascurabile (Improbabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Modifiche indesiderate dei dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?

Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Crittografia, Controllo degli accessi logici, Sicurezza dell'applicazione web, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Vulnerabilità, Backup

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?

Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Crittografia, Controllo degli accessi logici, Sicurezza dell'applicazione web, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Vulnerabilità,

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?

Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Limitato (Medio)

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce e alle fonti di rischio?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Importante (Probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Alto

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Perdita di dati

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

Attribuzione errata di un illecito, non attribuzione di un illecito commesso.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Hacker, malware, furto del dispositivo.

Quali sono le fonti di rischio?

Fonte umana esterna, fonte umana interna.

Quali misure fra quelle individuate contribuiscono a mitigare l'impatto (danno)?
Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Controllo degli accessi logici, Sicurezza dell'applicazione web, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Vulnerabilità, Backup

Quali misure fra quelle individuate contribuiscono a mitigare la probabilità?
Procedure per l'utilizzo delle notifiche digitali, Registro dei trattamenti, Tracciabilità, Archiviazione, Minimizzazione dei dati, Manutenzione, Gestione dei terzi che accedono ai dati (contratto con il responsabile del trattamento), Anonimizzazione, Politica di tutela della privacy, Formazione continua, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vigilanza sulla protezione dei dati, Lotta contro il malware, Certificazioni sulla sicurezza delle informazioni, Prevenzione delle fonti di rischio, Crittografia, Controllo degli accessi logici, Sicurezza dell'applicazione web, Gestione postazioni, Sicurezza dei canali informatici, Sicurezza dell'hardware, Vulnerabilità, Backup

Come stimereste la gravità del danno, specialmente alla luce degli impatti potenziali?
Alla luce degli impatti potenziali in relazione alla natura pregiudizievole del potenziale impatto dell'accesso illegittimo ai dati si ritiene che la gravità del rischio sia:

Trascurabile (Lieve)

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce e alle fonti di rischio?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Massimo (Altamente probabile)

Come stimereste il valore di base del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?
Alla luce dell'entità e della probabilità stimate che si concretizzi si ritiene che il valore del rischio sia stimabile di entità:

Medio

Alla luce delle misure tecniche e organizzative attualmente già implementate come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle misure attualmente implementate si ritiene che la probabilità del rischio sia stimabile di entità:

Trascurabile (Lieve)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste la probabilità di questo rischio (Modifiche indesiderate dei dati)?
Alla luce delle possibili fonti di rischio, delle caratteristiche e del livello di vulnerabilità del sistema e in considerazione delle minacce e delle fonti di rischio si ritiene che la probabilità del rischio sia stimabile di entità:

Limitato (Poco probabile)

Alla luce delle misure tecniche e organizzative attualmente già implementate come stimereste il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?
Alla luce delle misure tecniche e organizzative attualmente già implementate si ritiene che il valore del rischio sia stimabile di entità:

Basso

Alla luce del piano d'azione, come valutate la gravità di questo rischio (Modifiche indesiderate dei dati)?
Alla luce del piano di azione definito si ritiene che si otterrà una gravità del rischio stimabile di entità:

Trascurabile (Lieve)

Alla luce del piano d'azione, come valutate la probabilità di questo rischio (Modifiche indesiderate dei dati)?

Alla luce del piano di azione definito si ritiene che si otterrà una probabilità del rischio stimabile di entità:

Limitato (Poco probabile)

Alla luce del piano d'azione, come valutate il valore del rischio alla luce dell'entità e della probabilità stimate che si concretizzi?

Alla luce del piano di azione si ritiene che il valore del rischio sia stimabile di entità:

Basso

Data, 23.12.2025

Approvazione della valutazione di impatto da parte del Titolare del trattamento

Il Segretario Comunale designato ai trattamenti dei dati personali afferenti alle notifiche digitali
Dott. Umberto Bovenzi

(Firmato digitalmente)

In merito al parere sulla valutazione di impatto del tecnico che ha supportato il Titolare nella valutazione

Il tecnico
Liana Renacco

(Firmato digitalmente)

In merito al parere sulla valutazione di impatto del DPO/RDP

Il Responsabile della Protezione dei Dati Personali
Enrico Capirone

(Firmato digitalmente)