UNIONE DI COMUNI LOMBARDA
“UNIONE DEL DELMONA”
TRA I COMUNI DI PERSICO DOSIMO - GADESCO PIEVE DELMONA

ORIGINALE

Deliberazione della Giunta dell'Unione **n. 9 del 30 gennaio 2024**

OGGETTO: APPROVAZIONE VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) RELATIVA AI CANALI DI SEGNALAZIONE PER IL 'WHISTLEBLOWING'.

L'anno **duemilaventiquattro**, il giorno **trenta** del mese di **gennaio** alle ore **17:25**, in videoconferenza previo esaurimento delle formalità prescritte dalla Legge e dallo Statuto dell’Unione, si è riunita, sotto la presidenza del Presidente Achille Marelli, la Giunta dell’Unione del Delmona”. All’appello nominale risultano:

Cognome e Nome	**PRESENTI**	**ASSENTI**
MARELLI Achille	**P**	
BIGNARDI Giuseppe	**P**	
GRISI Doriana	**P**	
GUARNERI Enrica	**P**	
BARONE Riccardo		**A**
TOTALE	**4**	**1**

partecipa il Segretario Dell'Unione Matteo MALVICINI il quale provvede alla redazione del presente verbale.

Il Presidente, Achille MARELLI, riconosciuta legale l'adunanza, dichiara aperta la seduta ed invita la Giunta dell’Unione a trattare l'argomento di cui in oggetto.

OGGETTO: APPROVAZIONE VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) RELATIVA AI CANALI DI SEGNALAZIONE PER IL 'WHISTLEBLOWING'.

LA GIUNTA DELL'UNIONE

VISTI:
- la Deliberazione del Consiglio dell'Unione n. 25 del 15/12/2023 di approvazione della nota di aggiornamento al documento unico di programmazione (D.U.P.) per il periodo 2024-2026;
- la Deliberazione del Consiglio dell'Unione n. 26 del 15/12/2023 di approvazione del Bilancio di Previsione 2024-2026;
- la Deliberazione di Giunta dell'Unione n. 1 del 16/01/2024 con la quale è stato approvato il PEG 2024-2026;
- la Deliberazione di Giunta dell'Unione n. 6 del 30.01.2024 con la quale è stato approvato il PIAO 2024-2026;

VISTI:
- la Legge n. 190 del 6 novembre 2012 recante "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" con la quale è stato introdotto nell'Ordinamento italiano un sistema organico di disposizioni finalizzate alla prevenzione della corruzione e alla promozione dell'integrità in tutti i processi e le attività pubbliche;
- la Legge n. 179 del 30 novembre 2017 recante "Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato".
- La Direttiva (UE) 2019/1937 del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;
- Il D.lgs. 10/03/2023, 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" entrato in vigore il 30 marzo 2023 con efficacia dal 15 luglio 2023, in particolare gli articoli:
  Art. 1 Ambito di applicazione oggettivo Il presente decreto disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato. […].
  Art. 4 Canali di segnalazione interna I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali […], attivano, […] propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione […]"
  Art. 13. Trattamento dei dati personali […] 6 [I comuni …] 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. […]";

RILEVATO che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

CONSIDERATO che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:
- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e

organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

TENUTO PRESENTE che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

DATO ATTO che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

RILEVATO CHE, con il GDPR, è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

VISTO il D. lgs 196/2003, modificato dal D.Lgs. 10 agosto 2018 n. 101;

DATO ATTO CHE, 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 GDPR obbliga i titolari a svolgere:

- una "determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
- una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

TENUTO PRESENTE che la DPIA è una procedura prevista dall'art. 35 del Regolamento UE 206/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonchè i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;

TENUTO PRESENTE l'obbligo, in capo ai titolari, di consultare l'Autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

RILEVATO che la DPIA deve essere condotta prima di procedere al trattamento e che, deve comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari;

DATO ATTO CHE la responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione;

TENUTO PRESENTE che, ferma restando la discrezionalità dell'amministrazione nell'effettuare la determinazione preliminare e la valutazione di impatto, il Garante, con provvedimento n. 467 dell'11 ottobre 2018, ha reso pubblico l'Elenco delle tipologie di trattamenti da sottoporre OBBLIGATORIAMENTE a valutazione d'impatto, tra cui si menzionano:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3. Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;
4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni

elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .
8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

TENUTO PRESENTE che, ai sensi dell'art. 29 delle linee guida elaborate dal Gruppo di Lavoro 29 per la protezione dei dati, 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 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 per la cui definizione è stata condotta una DPIA

RILEVATO CHE, per quanto sopra, è necessario istituire:

1. una "Determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
2. una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

CONSIDERATO che:

- Il decreto legislativo 10 marzo 2023 n. 24, divenuto efficace il 15 luglio 2023, disciplina la materia del whistleblowing, abrogando le normative precedentemente in vigore in materia.
- Tale decreto disciplina la protezione delle persone che segnalano violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica *o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato"*.
- Il segnalante, peraltro, può fare la segnalazione, trovando la tutela fornita dal d.lgs. 24/2023, non solo durante il rapporto di lavoro, bensì anche prima che sia iniziato il rapporto stesso, qualora la segnalazione riguardi violazioni rilevate durante il processo di selezione o in altre fasi precontrattuali oppure durante il periodo di prova.
- La tutela è garantita anche nel caso di segnalazione fatta in seguito alla cessazione del rapporto di lavoro, sempreché la segnalazione riguardi una violazione di cui il segnalante è venuto a conoscenza nel corso del rapporto di lavoro.
- La novità di tale decreto risiede non tanto nella trattazione della materia, che peraltro veniva già precedentemente trattata, quanto nella tutela che viene apprestata alla figura del segnalante e alle altre figure che coadiuvano il segnalante.
- L'obiettivo di questo decreto non è solo quello di incentivare le segnalazioni, ma soprattutto di tutelare la riservatezza sull'identità del segnalante e delle persone coinvolte nella segnalazione.
- Un'altra importante novità che il decreto introduce riguarda la necessaria previsione di un canale di segnalazione interna, il quale deve prevedere più modalità di segnalazione, lasciando al segnalante la possibilità di scegliere quale utilizzare.

VISTA La delibera dell'ANAC Delibera n. 311 del 12 luglio 2023 – "Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne", che in particolare prevede:

"Paragrafo 3.1. – I canali interni

[…] Istituzione dei canali di segnalazione … Nell'atto organizzativo, adottato dall'organo di indirizzo, è opportuno che almeno vengano definiti:

- ➢ il ruolo e i compiti dei soggetti che gestiscono le segnalazioni;
- ➢ le modalità e i termini di conservazione dei dati, appropriati e proporzionati in relazione alla procedura di whistleblowing e alle disposizioni di legge. […]

I canali di segnalazione interna devono garantire la riservatezza, anche tramite il ricorso a strumenti di crittografia, ove siano utilizzati strumenti informatici:

- ➢ della persona segnalante;
- ➢ del facilitatore;
- ➢ della persona coinvolta o comunque dei soggetti menzionati nella segnalazione;
- ➢ del contenuto della segnalazione e della relativa documentazione.

Inoltre, al fine di agevolare il segnalante, a quest'ultimo va garantita la scelta fra diverse modalità di segnalazione:

- ➢ in forma scritta, anche con modalità informatiche (piattaforma online). La posta elettronica ordinaria e la PEC si ritiene siano strumenti non adeguati a garantire la riservatezza. Qualora si utilizzino canali e tecniche tradizionali, da disciplinare nell'atto organizzativo, è opportuno indicare gli strumenti previsti per garantire la riservatezza richiesta dalla normativa.
- ➢ in forma orale, alternativamente, attraverso linee telefoniche, con sistemi di messaggistica vocale, ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. […]"

DATO ATTO CHE il provvedimento, attuativo della direttiva europea 2019/1937, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato e prescrive l'obbligatorietà della DPIA per la gestione delle segnalazioni attraverso piattaforme esterne. Il trattamento di cui alla presente DPIA riguarda l'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo.

VISTI:

- il D.Lgs. 18 agosto 2000, n. 267, e successive modificazioni, recante: "Testo unico delle leggi sull'ordinamento degli enti locali";
- il vigente "Regolamento comunale sull'ordinamento degli uffici e dei servizi";
- la legge 7 agosto 1990, n. 241 e successive modificazioni, recante: "Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi";
- il D.Lgs. 30 giugno 2003, n. 196, recante: "Codice in materia di protezione dei dati personali", per quanto tuttora in vigore;
- il Regolamento UE 2016/679 del 27 aprile 2016 relativo alla "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati";
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;

- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto Comunale;
- Circolari e direttive del RPC;

RICHIAMATA la Delibera Giunta dell'Unione n. 101 del 15/12/2023 avente ad oggetto "Adesione al portale whistleblowing.it di Transparency International. Adeguamento al decreto legislativo 10 marzo 2023, n. 24 – Approvazione regolamento segnalazione – Modifica PIAO, sottosezione rischi corruttivi e trasparenza";

RITENUTO, per le motivazioni che precedono, di approvare la Valutazione d'impatto sulla protezione dei dati (DPIA) relativa all'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo, ai sensi del Regolamento (UE) n.679/2016 e del D.Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

DATO ATTO CHE il responsabile del procedimento, è il Segretario dell'Unione e che lo stesso, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità dei trattamenti oggetto di DPIA, nonché delle misure tecniche e organizzative individuate dai titolari per mitigare l'impatto del trattamento, è tenuto a garantire la conoscibilità della Valutazione d'impatto sulla protezione dei dati (DPIA) a tutti i dipendenti dell'Ente;

VISTO il parere favorevole espresso dal Segretario dell'Unione, in qualità di Responsabile del Servizio amministrativo in ordine alla regolarità del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

DATO ATTO che dal presente provvedimento non derivano impatti economici o patrimoniali a carico del bilancio dell'Ente e che dunque non risulta necessaria l'espressione del parere di regolarità contabile del Responsabile del Servizio finanziario ai sensi e per gli effetti degli artt. 49 del D.Lgs. 18.08.2000, n. 267;

CON VOTI unanimi favorevoli, resi nelle forme di legge

DELIBERA

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. **DI APPROVARE** la Valutazione d'impatto sulla protezione dei dati (DPIA) relativa all'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo, ai sensi del Regolamento (UE) n.679/2016 e del D.Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

2. **DI DISPORRE** che al presente provvedimento venga assicurata:
   a) la pubblicità legale con pubblicazione all'Albo Pretorio per 15 gg. consecutivi;
   b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";

3. **DI DARE ATTO** che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.Lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.Lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.

4. **DI DISPORRE** che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.Lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

5. **DI DARE ATTO**, ai sensi dell'art. 3 della Legge n. 241/90 e ss.mm.ii. sul procedimento amministrativo, che qualunque soggetto ritenga il presente atto illegittimo e si ritenga dallo stesso direttamente leso, può proporre ricorso innanzi al Tribunale Amministrativo Regionale, Sezione di Brescia, al quale è possibile presentare i propri rilievi in ordine alla legittimità del presente atto, entro e non oltre 60 giorni dall'ultimo di pubblicazione all'Albo on line;

6. **DI COMUNICARE** la presente deliberazione ai capigruppo consiliari ai sensi dell'art.125, comma 1 del D.lgs 18 agosto 2000 n.267;

Con separata successiva votazione unanime

7. **DI RENDERE** il presente atto immediatamente eseguibile ai sensi dell’art. 134 – 4° comma – D. Lgs. 18.08.2000 n° 267.

UNIONE DI COMUNI LOMBARDA
"UNIONE DEL DELMONA"
PROVINCIA DI CREMONA

DPIA

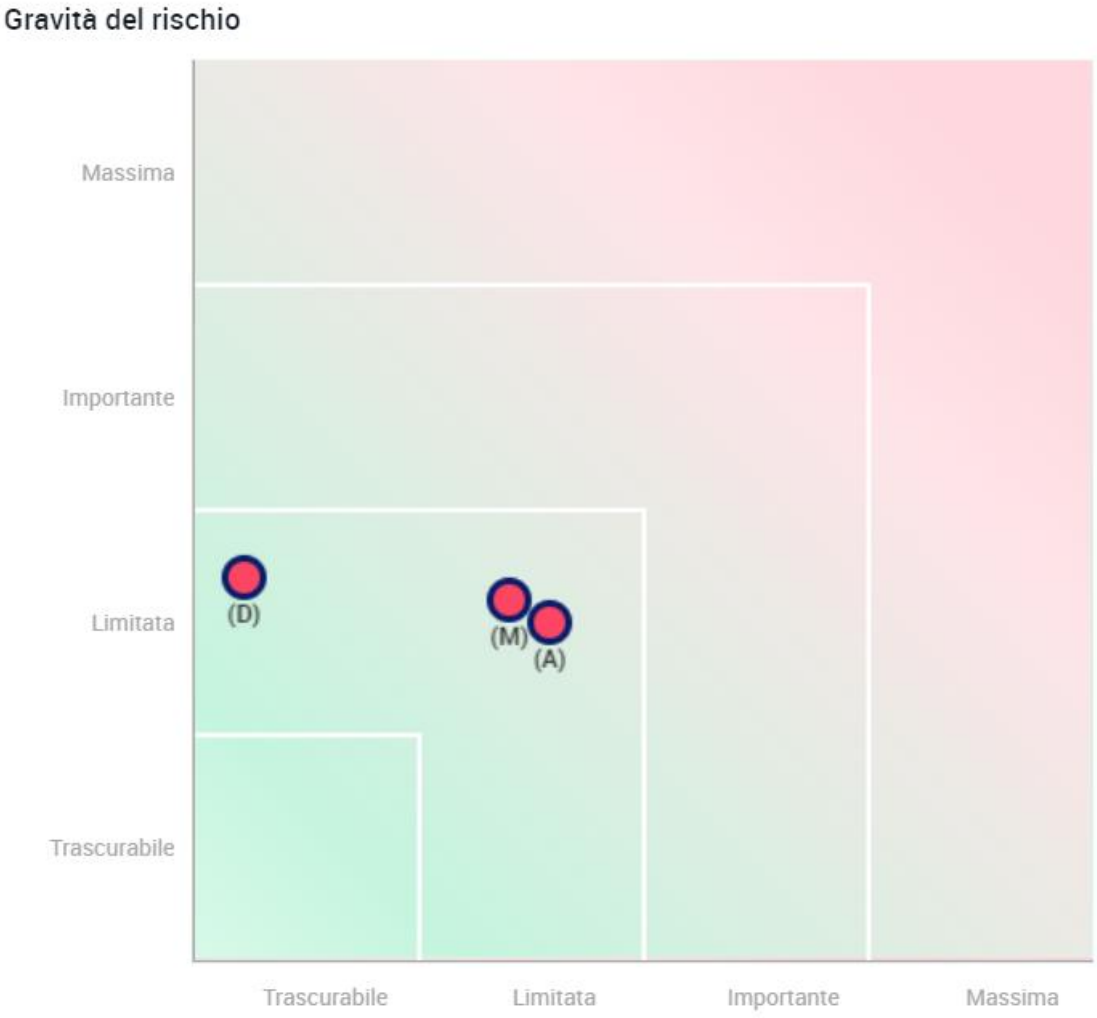
RELATIVA ALL'INTRODUZIONE DI UNA PIATTAFORMA PER IL WHISTLEBLOWING

WHISTLEBLOWING SOLUTIONS

(MEDIANTE UTILIZZO DEL SOFTWARE P.I.A.)

Approvato con Deliberazione di Giunta n. 9 del 30/01/2024

MAPPATURA DEL RISCHIO



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

PIANO D'AZIONE DEL RISCHIO

Panoramica

CONTESTO

Panoramica del trattamento

Il trattamento di cui alla presente DPIA riguarda l'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo. Il **decreto legislativo n. 24/2023**, che introduce la nuova disciplina del **whistleblowing** in Italia, è entrato in vigore il 30 marzo 2023. Il provvedimento, attuativo della **direttiva europea 2019/1937**, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato. Il Comune ha deciso di introdurre il proprio canale di segnalazioni interne avvalendosi di **WhistleblowingPA,** un progetto di **Transparency International Italia** e di **Whistleblowing Solutions Impresa Sociale**.

Le figure soggettive connesse al trattamento

Titolare del Trattamento è l'Unione di Comuni Lombarda "Unione del Delmona"

Responsabile Esterno del Trattamento è Whistleblowing Solutions I.S. S.r.l., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961 del legale rappresentante pro tempore Ing. Giovanni Pellerano. La Società è stata nominata Responsabile esterno del trattamento ai sensi dell'art. 28 Reg. UE 679/16.

Data Protection Officer è Avv. Alessia Roberto, Via Sauli n. 39/11, Genova (GE) che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente indirizzo e-mail aroberto.legale@gmail.com.

Incaricato del trattamento, per espressa previsione di legge, in quanto Responsabili della Prevenzione della Corruzione e Trasparenza è il Segretario dell'Unione di Comuni Lombarda "Unione del Delmona" Dr. Matteo Malvicini, in quanto persona fisica avente l'accesso esclusivo all'indirizzo e-mail al quale pervengono tutte le segnalazioni.

Gli standard applicabili al trattamento

Al trattamento in si applicano le seguenti **normative e provvedimenti**:

- Regolamento UE n. 2016/679 (GDPR);

- D.Lgs. n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.Lgs. 101/2018;

- Il D. Lgs. 10 marzo 2023, n. 24 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del

Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

Standard applicabili:

- ISO27001 “Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks”

- ISO27017 controlli di sicurezza sulle informazioni

- ISO27018 per la protezione dei dati personali nei servizi Public Cloud

- Qualifica AGID

- Certificazione CSA Star

Dati, processi e risorse di supporto

Tipologia dei dati trattati

I dati trattati sono quelli che riguardano le procedure di segnalazione di cui al d. lgs. n. 24 del 2023: l'identità del segnalante, il contenuto della segnalazione di violazione di norme di legge anche eurounitarie e l'identità del soggetto a cui la segnalazione si riferisce. In virtù del Contratto di servizio il Fornitore esegue operazioni di trattamento di dati personali (di seguito, "Dati Personali") di titolarità del Committente, e riferiti unicamente ai dati necessari per l’erogazione dei servizi pattuiti tra le parti. In particolare l’acquisizione e l’archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

Il ciclo di vita del trattamento dei dati

I dati trattati sono quelli che riguardano le procedure di segnalazione di cui al d. lgs. n. 24 del 2023: l'identità del segnalante, il contenuto della segnalazione di violazione di norme di legge anche eurounitarie e l'identità del soggetto a cui la segnalazione si riferisce. In virtù del Contratto di servizio il Fornitore esegue operazioni di trattamento di dati personali (di seguito, "Dati Personali") di titolarità del Committente, e riferiti unicamente ai dati necessari per l’erogazione dei servizi pattuiti tra le parti. In particolare l’acquisizione e l’archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o

identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

1) Attivazione della piattaforma 2) Configurazione della piattaforma 3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti 4) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Periodo di conservazione dei dati Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Le risorse di supporto ai dati

Il Sistema di WhistelblowingPA si avvale di un Software di whistleblowing professionale GlobaLeaks Infrastruttura IaaS e SaaS privata basata su tecnologie: - Dettaglio Hardware - VMWARE (virtualizzazione) - Debian Linux LTS (sistema operativo) - VEEAM (backup) - OPNSENSE (firewall) - OPENVPN (vpn).

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento dei dati

Gli scopi del trattamento sono specifici, espliciti e legittimi, in quanto i dati personali sono raccolti e trattati dal Comune esclusivamente per consentire agli interessati di effettuare le segnalazioni previste dal d. lgs n. 24 del 2023 (c.d. normativa sul whistleblowing).

Le basi legali che rendono lecito il trattamento

Il trattamento è lecito, ai sensi dell'art. 6, lett. a) del GDPR, in quanto l'interessato effettuando la segnalazione esprime implicitamente il proprio consenso al trattamento dei propri dati personali

Il trattamento è lecito, ai sensi dell'art. 6, lett. c) del GDPR, in quanto il Titolare del trattamento deve effettuarlo per adempiere agli obblighi legali previsti dal diritto dell'Unione (direttiva europea 2019/1937) e dal diritto dello Stato italiano (d. lgs. 24 del 2023)

Il trattamento è lecito, ai sensi dell'art. 6, lett. e) del GDPR, in quanto il trattamento è necessario per l'esecuzione dei compiti di interesse pubblico legati alla normativa anticorruzione di cui è investito il Titolare.

Adeguatezza, pertinenza e limiti: la minimizzazione dei dati

In applicazione del principio della pertinenza, le segnalazioni raccolte e l'identità del segnalante vengono raccolti in base a quanto rappresentato dal whistleblower. Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email 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. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Esattezza ed aggiornamento dei dati

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.

Periodo di conservazione dei dati

La policy di *data retention* di *default* delle segnalazioni è di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.

Il sistema prevede la cancellazione dell'intera piattaforma passati n. 15 giorni dalla disattivazione del servizio.

Misure a tutela dei diritti degli interessati

L'informativa agli interessati

Gli interessati al trattamento sono informati tramite un'informativa liberamente consultabile sia sull'Amministrazione Trasparente dell'Unione che sul sito internet del Responsabile esterno (https://www.whistleblowing.it/assistenza/).

Modalità di ottenimento del consenso

Dato atto che per consenso dell'interessato si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; è lo stesso interessato effettuando la segnalazione ad esprimere implicitamente il proprio consenso al trattamento dei propri dati personali.

Esercizio del diritto di accesso e portabilità dei dati

Coloro che effettuano la segnalazione hanno diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e altre informazioni specificate nell'art. 15 del GDPR.

Ai sensi dell'art. 20 del GDPR gli interessati hanno il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che li riguardano forniti a un titolare del trattamento e hanno il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento.

A tal fine possono utilizzare i seguenti recapiti PEC: unione.delmona@pec.regione.lombardia.it – mail: info@unionedelmona.cr.it.

Esercizio dei diritti di rettifica e cancellazione

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi di cui all'art. 17 GDPR.

A tal fine si possono utilizzare i seguenti recapiti PEC: unione.delmona@pec.regione.lombardia.it – mail: info@unionedelmona.cr.it.

Esercizio dei diritti di limitazione e opposizione

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi di cui all'art. 18 del GDPR e può opporsi al trattamento in essere nel rispetto dell'art. 21 del GDPR.

A tal fine si possono utilizzare i seguenti recapiti PEC: unione.delmona@pec.regione.lombardia.it – mail: info@unionedelmona.cr.it.

Responsabili esterni del trattamento e trasferimento dati al di fuori dell'UE

Gli obblighi del Responsabile esterno sono definiti tramite contratto sottoscritto dal legale rappresentante dell'Ente. Tali obblighi riguardano, oltre la Whistleblowing Solutions in qualità di Responsabile del trattamento, i seguenti soggetti: Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions e Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions).

RISCHI

Misure di prevenzione esistenti o pianificate

1) Crittografia

L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington. Ogni informazione scambiata viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+. Ogni informazione circa le segnalazioni e i relativi metadati registrata dal sistema viene protetta con chiave asimmetrica personale e protocollo a curve ellittiche per ciascun utente avente accesso al sistema e ai dati delle segnalazioni. Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento Il sistema è installato su sistema operativo Linux su cui è attiva Full Disk Encryption (FDE) a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto. Protocollo crittografico: https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html.

2) Controllo degli accessi logici

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.

3) Tracciabilità

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing. I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent. I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

4) Archiviazione

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.

5) Controlli sulle vulnerabilità

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

6) Backup

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

7) Manutenzione

E' 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 Whistleblowing Solutions 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 Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

8) Sicurezza dei canali informatici

Tutte le connessioni sono protette tramite protocollo TLS 1.2+ Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

9) Sicurezza dell'hardware

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24. I datacenter del fornitore IaaS sono certificati ISO27001.

10) Gestione incidenti di sicurezza e violazioni dei dati personali

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

11) Lotta contro i malware

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati 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 tematica tramite formazione diretta o documentazione online.

12) Minimizzazione dei dati e anonimato

Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e

dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

RISCHI MAPPATI

a) ACCESSO ILLEGITTIMO AI DATI

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

Azioni ritorsive nei confronti del segnalante e pregiudizio alla sua reputazione.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

accesso non autorizzato ai sistemi del Comune per operazioni non consentite/non autorizzate, azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Sicurezza dell'hardware, Minimizzazione dei dati e anonimato, Controlli sulle vulnerabilità.

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, le misure individuate, pianificate ed adottate contribuiscono a mitigare la gravità dei rischi individuati.

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

Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

RISCHI MAPPATI

b) MODIFICHE INDESIDERATE DEI DATI

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

Azioni ritorsive nei confronti del segnalante, impossibilità di portare a compimento la procedura di segnalazione volta ad impedire fenomeni di *mala gestio* della cosa pubblica.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Archiviazione, Backup, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Sicurezza dell'hardware, Sicurezza dei canali informatici, Vulnerabilità, Crittografia, Manutenzione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?

Limitata, le misure individuate, pianificate ed adottate contribuiscono a mitigare la gravità dei rischi individuati.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?

Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

RISCHI MAPPATI

c) PERDITA DI DATI

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Impossibilità di portare a compimento la procedura di segnalazione volta ad impedire fenomeni di *mala gestio* della cosa pubblica.

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Accesso non autorizzato ai sistemi del Comune per operazioni non consentite/non autorizzate, azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio, furto o distruzione degli hardware.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio, incidente o un sinistro verificatosi presso uno dei soggetti preposti al trattamento.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

Manutenzione, Archiviazione, Backup, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione degli incidenti di sicurezza e delle violazioni dei dati personali.

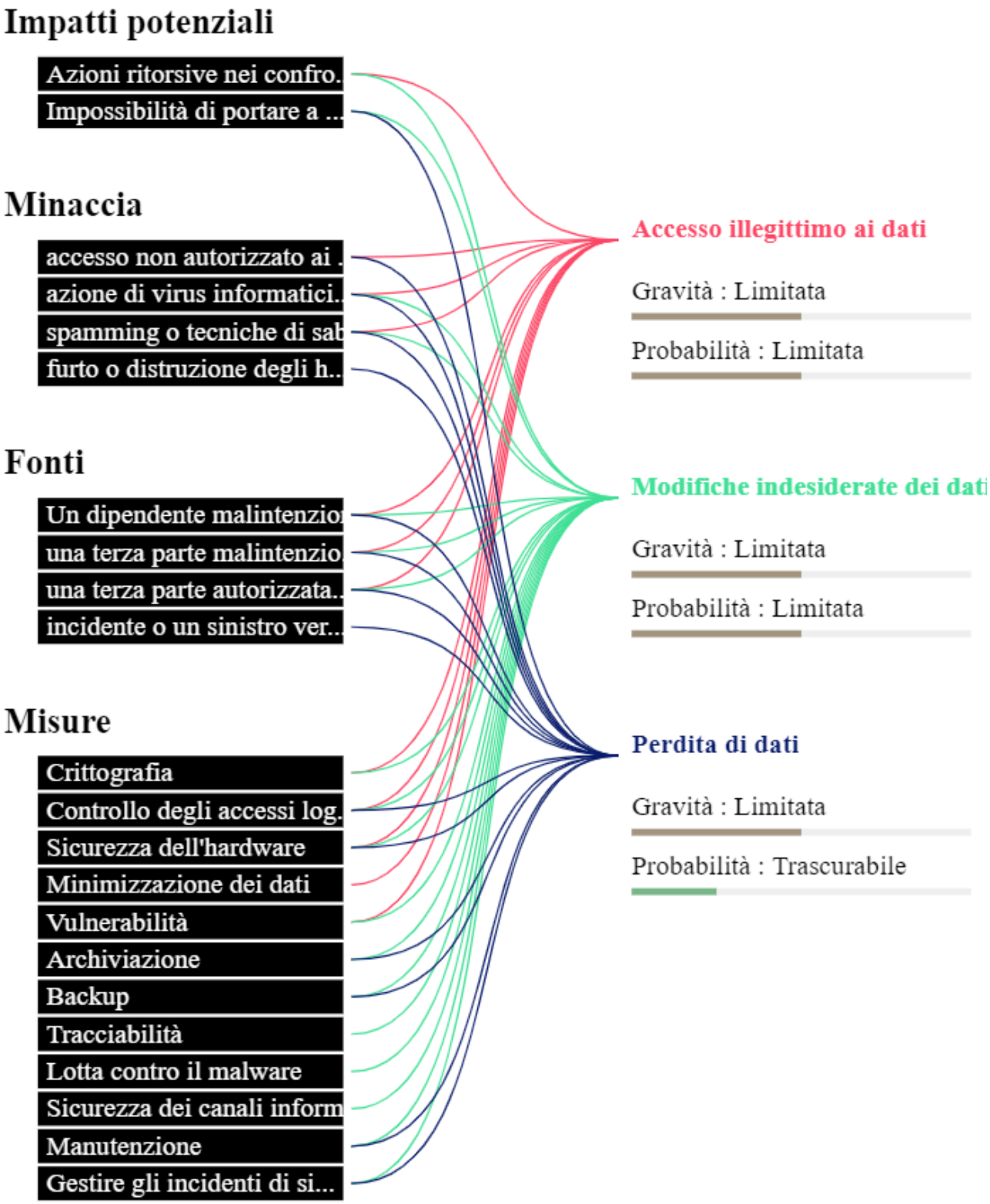
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la gravità i rischi individuati

Come stimereste la Probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

Panoramica dei rischi



VALIDAZIONE

Nome del DPO

Avv. Alessia Roberto

Parere del DPO/RPD

Il trattamento appare adeguato. Il Titolare del Trattamento ha previsto una nuova soluzione organizzativa che prevede l'uso di nuove tecnologie che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Titolare ha correttamente effettuato la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. La valutazione d'impatto è sufficientemente strutturata, e dà conto dei probabili rischi, che sono valutati ed adeguatamente mitigati dalle soluzioni adottate. In particolare, A seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati, a seguito dell'adozione delle misure di mitigazione del rischio indicate dall'ente, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto. Il sistema nel suo complesso coniuga in un ragionevole equilibrio il diritto alla riservatezza e protezione dei dati personali dei soggetti interessati con le attività di gestione dei trattamenti connessi allo 'whistleblowing', come da disposizioni normative.

Pertanto nel complesso, alla data odierna, non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 GDPR; per tale ragione, inoltre, non si rende necessario procedere con la Consultazione preventiva ex art. 36 GDPR.

Richiesta del parere degli interessati

Non è stato chiesto il parere di interessati esterni perché non si sono individuate tali figure in modo chiaro e preciso perché la predisposizione del canale interno per le segnalazioni è un obbligo di legge (d. lgs. n. 24 del 2023) a cui la PA non può sottrarsi.

Gadesco Pieve Delmona, il __/__/2024

DPO

Dell'Unione del Delmona

Avv. Alessia Roberto

_____

UNIONE DI COMUNI LOMBARDA
“UNIONE DEL DELMONA”
TRA I COMUNI DI PERSICO DOSIMO - GADESCO PIEVE DELMONA

Proposta di deliberazione della Giunta dell'Unione ad oggetto:

APPROVAZIONE VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) RELATIVA AI CANALI DI SEGNALAZIONE PER IL 'WHISTLEBLOWING'.

Parere di regolarità tecnica attestante la regolarità e la correttezza dell'azione amministrativa.

Il sottoscritto, in qualità di SEGRETARIO DELL'UNIONE, ai sensi dell’art. 49,comma 1, e 147 bis, comma1 del T.U. approvato con D.Lgs. 18.08.2000, n. 267, esprime PARERE FAVOREVOLE in ordine alla regolarità tecnica e alla correttezza amministrativa della proposta di provvedimento indicato in oggetto.

Lì, 26.01.2024

SEGRETARIO DELL'UNIONE

Matteo MALVICINI

Originale

Letto, confermato e sottoscritto.

IL PRESIDENTE	IL SEGRETARIO DELL'UNIONE
Dott. Achille MARELLI	Matteo MALVICINI

ADEMPIMENTI RELATIVI ALLA PUBBLICAZIONE

Si attesta:

- che copia della presente deliberazione viene pubblicata all'albo il giorno giovedì 1 febbraio 2024 e vi rimarrà per 15 giorni consecutivi.

- è stata comunicata in data odierna ai Capigruppo Consiliari ai sensi dell'art. 125 D.Lgs. n. 18.08.2000 n° 267.

Lì, giovedì 1 febbraio 2024

IL SEGRETARIO DELL'UNIONE

Matteo MALVICINI

ESECUTIVITA' DELLA DELIBERAZIONE

Il sottoscritto Segretario Dell'Unione, visti gli atti d'ufficio, attesto che la presente deliberazione:

[X] è stata dichiarata immediatamente eseguibile, ex. art. 134, 4° comma, T.U. D.Lgs. 267/2000;

[ ] è divenuta esecutiva dopo il decimo giorno dalla pubblicazione, ex. art. 134, 3° comma del T.U. D.Lgs. 267/2000;

Addì, _____

IL SEGRETARIO DELL'UNIONE

Matteo MALVICINI