DELIBERAZIONE DELLA GIUNTA UNIONE

JNIONE LOMBARDA DEI COMUNI MUNICIPI/

PROVINCIA DI CREMONA

☐ Comunicata ai Capigruppo Consiliari

il Nr. Prot.

C O P I A

ADESIONE AL PORTALE WHISTLEBLOWING DI TRANSPARENCY INTERNATIONAL ED APPROVAZIONE RELATIVA DOCUMENTAZIONE - ADEGUAMENTO AL DECRETO LEGISLATIVO 10 MARZO 2023 N. 24.

Nr. Progr. **14**

Data **21/02/2024**

Nr. Prot.

Seduta Nr. **2**

Cod. Materia: *Cod. Ente : 019061*

L'anno DUEMILAVENTIQUATTRO questo giorno VENTUNO del mese di FEBBRAIO alle ore 14:00 convocata con le prescritte modalità, in modalità MISTA: presso il Municipio di MOTTA BALUFFI e

Fatto l'appello nominale risultano:

Cognome e Nome	***Carica***	***Presente***
Oliva Ennio Roberto	PRESIDENTE	Presente
Premoli Antonietta	ASSESSORE	Presente
Zapponi Riccardo	ASSESSORE	Presente
Capelli Floriana	ASSESSORE	Presente
POLI Federico	ASSESSORE	Assente
Marca Antonella	ASSESSORE	Assente
Totale Presenti **4**	***Totale Assenti***	**2**

Assenti giustificati i signori:
POLI FEDERICO; MARCA ANTONELLA

Assenti NON giustificati i signori:

Nessun convocato risulta assente ingiustificato

Partecipa il SEGRETARIO UNIONE, Nanni Maria Rita.

Il Sig. OLIVA ENNIO ROBERTO in qualità di PRESIDENTE assume la presidenza e, constatata la legalità dell'adunanza, dichiara aperta la seduta invitando la Giunta Unione a deliberare sull'oggetto sopra indicato.

DELIBERAZIONE DELLA GIUNTA UNIONE NR. 14 DEL 21/02/2024

OGGETTO:

ADESIONE AL PORTALE WHISTLEBLOWING DI TRANSPARENCY INTERNATIONAL ED APPROVAZIONE RELATIVA DOCUMENTAZIONE - ADEGUAMENTO AL DECRETO LEGISLATIVO 10 MARZO 2023 N. 24.

Si dà atto che la presente seduta di GIUNTA UNIONE è stata convocata in modalità mista secondo il REGOLAMENTO PER LO SVOLGIMENTO IN MODALITA' TELEMATICA DELLE SEDUTE DEL CONSIGLIO UNIONE E DELLA GIUNTA UNIONE - in particolare l'art.8 c.1 che recita testualmente: Le sedute del Consiglio/Giunta possono svolgersi anche in forma mista, con la simultanea e contestuale partecipazione sia in presenza fisica, negli ambienti a tal fine dedicati, che mediante collegamento alla piattaforma informatica.

Alla seduta odierna risultano pertanto presenti

MODALITA' PRESENZA: OLIVA R., PREMOLI A. CAPELLI F.

MODALITA' VIDEOCONFERENZA: ZAPPONI R.

LA GIUNTA UNIONE

RICHIAMATE:

- 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";

VISTO il Decreto legislativo 10 marzo 2023, n. 24, che recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione;

VISTO lo schema delle linee guida dell'Autorità Nazionale Anticorruzione previste dall'art. 10 del d.lgs. 24/2023;

VISTO l'art. 1 del D.lgs. 24/2023, a tenore del quale:

"*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. Le disposizioni del presente decreto non si applicano: a) alle*

contestazioni, rivendicazioni o richieste legate ad un interesse di carattere personale della persona segnalante o della persona che ha sporto una denuncia all'autorità giudiziaria o contabile che attengono esclusivamente ai propri rapporti individuali di lavoro o di impiego pubblico, ovvero inerenti ai propri rapporti di lavoro o di impiego pubblico con le figure gerarchicamente sovraordinate; b) alle segnalazioni di violazioni laddove già disciplinate in via obbligatoria dagli atti dell'Unione europea o nazionali indicati nella parte II dell'allegato al presente decreto ovvero da quelli nazionali che costituiscono attuazione degli atti dell'Unione europea indicati nella parte II dell'allegato alla direttiva (UE) 2019/1937, seppur non indicati nella parte II dell'allegato al presente decreto; c) alle segnalazioni di violazioni in materia di sicurezza nazionale, nonché di appalti relativi ad aspetti di difesa o di sicurezza nazionale, a meno che tali aspetti rientrino nel diritto derivato pertinente dell'Unione europea. 3. Resta ferma l'applicazione delle disposizioni nazionali o dell'Unione europea in materia di: a) informazioni classificate; b) segreto professionale forense e medico; c) segretezza delle deliberazioni degli organi giurisdizionali. 4. Resta altresì ferma l'applicazione delle disposizioni di procedura penale, di quelle in materia di autonomia e indipendenza della magistratura, delle disposizioni sulle funzioni e attribuzioni del Consiglio superiore della magistratura, comprese le relative procedure, per tutto quanto attiene alla posizione giuridica degli appartenenti all'ordine giudiziario, oltre che in materia di difesa nazionale e di ordine e sicurezza pubblica di cui al regio decreto, 18 giugno 1931, n. 773, recante il testo unico delle leggi di pubblica sicurezza. Resta altresì ferma l'applicazione delle disposizioni in materia di esercizio del diritto dei lavoratori di consultare i propri rappresentanti o i sindacati, di protezione contro le condotte o gli atti illeciti posti in essere in ragione di tali consultazioni, di autonomia delle parti sociali e del loro diritto di stipulare accordi collettivi, nonché di repressione delle condotte antisindacali di cui all'articolo 28 della legge 20 maggio 1970, n. 300.";

VISTO l'art. 4 del D.lgs. 24/2023, a mente del quale:

"I soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano, ai sensi del presente articolo, 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, nonché del contenuto della segnalazione e della relativa documentazione. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto. 2. La gestione del canale di segnalazione e' affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero e' affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato. 3. Le segnalazioni sono effettuate in forma scritta, anche con modalità informatiche, oppure in forma orale. Le segnalazioni interne in forma orale sono effettuate attraverso linee telefoniche o sistemi di messaggistica vocale ovvero, su richiesta della persona segnalante, mediante un incontro diretto fissato entro un termine ragionevole. 4. I comuni diversi dai capoluoghi di provincia possono condividere il canale di segnalazione interna e la relativa gestione. I soggetti del settore privato che hanno impiegato, nell'ultimo anno, una media di lavoratori subordinati, con contratti di lavoro a tempo indeterminato o determinato, non superiore a duecentoquarantanove, possono condividere il canale di segnalazione interna e la relativa gestione. 5. I soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna. 6. La segnalazione interna presentata ad un soggetto diverso da quello indicato nei commi 2, 4 e 5 e'

trasmessa, entro sette giorni dal suo ricevimento, al soggetto competente, dando contestuale notizia della trasmissione alla persona segnalante";

DATO ATTO che:

- il Piano Nazionale Anticorruzione (PNA), approvato con la deliberazione n. 72 dell'11settembre 2013 dall'Autorità Nazionale Anticorruzione, riconduce espressamente la tutela del dipendente che segnala condotte illecite, tra le azioni e misure generali finalizzate alla prevenzione della corruzione, in particolare fra quelle obbligatorie;
- il sistema di prevenzione della corruzione introdotto dalla legge 190/2012 deve realizzarsi attraverso un'azione coordinata tra un livello nazionale ed uno "decentrato";
- il PNA impone alle pubbliche amministrazioni, di cui all'art. 1, comma 2, del D.Lgs 165/2001, l'assunzione dei "necessari accorgimenti tecnici per dare attuazione alla tutela del dipendente che effettua le segnalazioni".

RICHIAMATA la delibera di Giunta Unione di approvazione del Piano Integrato di Attività e Organizzazione – PIAO;

PRESO ATTO che l'ente, in ossequio alle prescrizioni di cui al decreto legislativo 10 marzo 2023, n. 24, che recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, intende aderire al progetto *Whistleblowing PA*, nato dalla volontà di *Transparency International Italia* di offrire a tutte le Pubbliche Amministrazioni un software informatico gratuito (disponibile al link *whistleblowing.it*) per dialogare con i segnalanti, grazie a modalità che garantiscono l'anonimato;

RITENUTO pertanto opportuno aderire a tale modalità di gestione informatizzata delle segnalazioni predette, anche nell'ottica di garantire in maniera completa la riservatezza del segnalante nella procedura informatizzata sin dalla fase di avvio delle segnalazioni, riservandosi di aggiornare la relativa sezione del PIAO – sottosezione rischi corruttivi e trasparenza;

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;

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;

VISTA la Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale e ritenuta la stessa meritevole di approvazione;

DATO ATTO che il RPCT dell'ente Unione Municipia , 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;

VISTA l' informativa ai sensi degli art. 13 - 14 del GDPR 2016/679 whistleblowing - soggetti che segnalano illeciti d.lgs 24/2023 e ritenuta la stessa meritevole di approvazione, allegata al presente atto;

RICONOSCIUTA la piena competenza della Giunta a deliberare sulla materia in oggetto;

APPURATO che dall'adozione del presente atto non derivano oneri, diretti o indiretti;

VISTI:

- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;

- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Statuto Unione;
- Regolamento di organizzazione degli uffici e dei servizi;

ACQUISITO, conseguentemente, il solo parere favorevole di regolarità tecnica del Segretario espresso in qualità di RPCT;

CON VOTI favorevoli n. 04 contrari n. 0 ed astenuti n. 0 resi nelle forme di legge come segue:

- per alzata di mano da parte dei componenti presenti nella sala: favorevoli n. 03, contrari n. 0 ed astenuti n. 0

- per appello nominale, mediante affermazione vocale-audio, da parte dei componenti collegati in videoconferenza: favorevoli n. 01, contrari n. 0 ed astenuti n. 0

DELIBERA

1- **DI ADERIRE**, in ossequio alle prescrizioni di cui al decreto legislativo 10 marzo 2023, n. 24, che recepisce in Italia la Direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019, al progetto *Whistleblowing PA* curato da *Transparency International Italia;*

2- **DI DEMANDARE** al Segretario unione in qualità di RPC, l'attuazione di quanto in questa sede deliberato e, in particolare, la formulazione delle istruzioni operative da impartire alla struttura dell'ente nell'ottica di consentire l'utilizzo della piattaforma telematica gratuitamente resa disponibile per il tramite di *Transparency International Italia* e disponibile al link *whistleblowing.it*;

3- **DI APPROVARE** la Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, allegata alla presente, per formarne parte integrante e sostanziale;

4- **DI APPROVARE** l'informativa ai sensi degli art. 13 - 14 del GDPR 2016/679 whistleblowing - soggetti che segnalano illeciti D.Lgs 24/2023 che si allega al presente atto quale parte integrante e sostanziale;

5- **DI TRASMETTERE** la presente alle OOSS e alle RSU per opportuna conoscenza;

4- **DI DARE** ampia diffusione al personale comunale dell'approvazione della presente deliberazione;

2**. DI DISPORRE** che al presente provvedimento venga assicurata:

a) la pubblicità legale con pubblicazione all'Albo Pretorio;

b) l'invio ai dipendenti dell'Ente;

nonché

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";

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 DICHIARARE**, con successiva e unanime votazione, la presente immediatamente esecutiva, stante l'urgenza di provvedere.

CON VOTI favorevoli n. 04 contrari n. 0 ed astenuti n. 0 resi nelle forme di legge come segue:

- per alzata di mano da parte dei componenti presenti nella sala: favorevoli n. 03, contrari n. 0 ed astenuti n. 0

- per appello nominale, mediante affermazione vocale-audio, da parte dei componenti collegati in videoconferenza: favorevoli n. 01, contrari n. 0 ed astenuti n. 0

Letto, approvato e sottoscritto.

IL PRESIDENTE
F.to OLIVA ENNIO ROBERTO

IL SEGRETARIO UNIONE
F.to NANNI MARIA RITA

Attesto che la presente deliberazione verrà pubblicata all'Albo comunale il **14/03/2024** e vi rimarrà per 15 giorni consecutivi.

Data: 14/03/2024

IL SEGRETARIO UNIONE
F.to NANNI MARIA RITA

Attesto che la presente deliberazione è conforme all'originale.

Data: 14/03/2024

IL SEGRETARIO UNIONE
NANNI MARIA RITA

La presente deliberazione è stata dichiarata immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del D. Lgs. 18 agosto 2000, n. 267, il giorno **21/02/2024**.

Data: 21/02/2024 00:00:00

IL SEGRETARIO UNIONE
F.to NANNI MARIA RITA

La presente deliberazione è divenuta esecutiva decorsi 10 giorni dalla pubblicazione, ai sensi dell'art. 134, comma 3, del D. Lgs. 18 agosto 2000, n. 267, il giorno **24/03/2024**.

Data: 24/03/2024

IL SEGRETARIO UNIONE
F.to NANNI MARIA RITA

UNIONE LOMBARDA DEI COMUNI MUNICIPIA

PROVINCIA DI CREMONA

DELIBERAZIONE DELLA GIUNTA UNIONE

Delibera nr. **14** Data Delibera **21/02/2024**

OGGETTO

ADESIONE AL PORTALE WHISTLEBLOWING DI TRANSPARENCY INTERNATIONAL ED APPROVAZIONE RELATIVA DOCUMENTAZIONE - ADEGUAMENTO AL DECRETO LEGISLATIVO 10 MARZO 2023 N. 24.

PARERI DI CUI ALL' ART. 49, C. 2 E 97, C.4.B. DEL T.U. N. 267/2000 E SUCCESSIVE MODIFICAZIONI

IL RESPONSABILE DEL SERVIZIO	Per quanto concerne la REGOLARITA' TECNICA esprime parere : **FAVOREVOLE** Data 19/02/2024 **SEGRETARIO UNIONE** *F.to Nanni Maria Rita*

PARERI DI CUI ALL' ART. 49, C. 1 DEL T.U. N. 267/2000 E SUCCESSIVE MODIFICAZIONI

IL RESPONSABILE DEL SERVIZIO FINANZIARIO	Per quanto concerne la REGOLARITA' CONTABILE esprime parere : Data

D.P.I.A.

Data Protection Impact Assessment Trattamento Whistleblowing

TITOLARE DEL TRATTAMENTO: **UNIONE MUNICIPIA**

AREA/SETTORE/SERVIZIO: **AMMINISTRATIVA-AFFARI GENERALI**

DIRIGENTE/RESPONSABILE: SEGRETARIO UNIONE

DATA CREAZIONE DEL DOCUMENTO: 16/02/2024

RESPONSABILE PROTEZIONE DATI: DOTT.SSA SIMONA PERSI

SOMMARIO

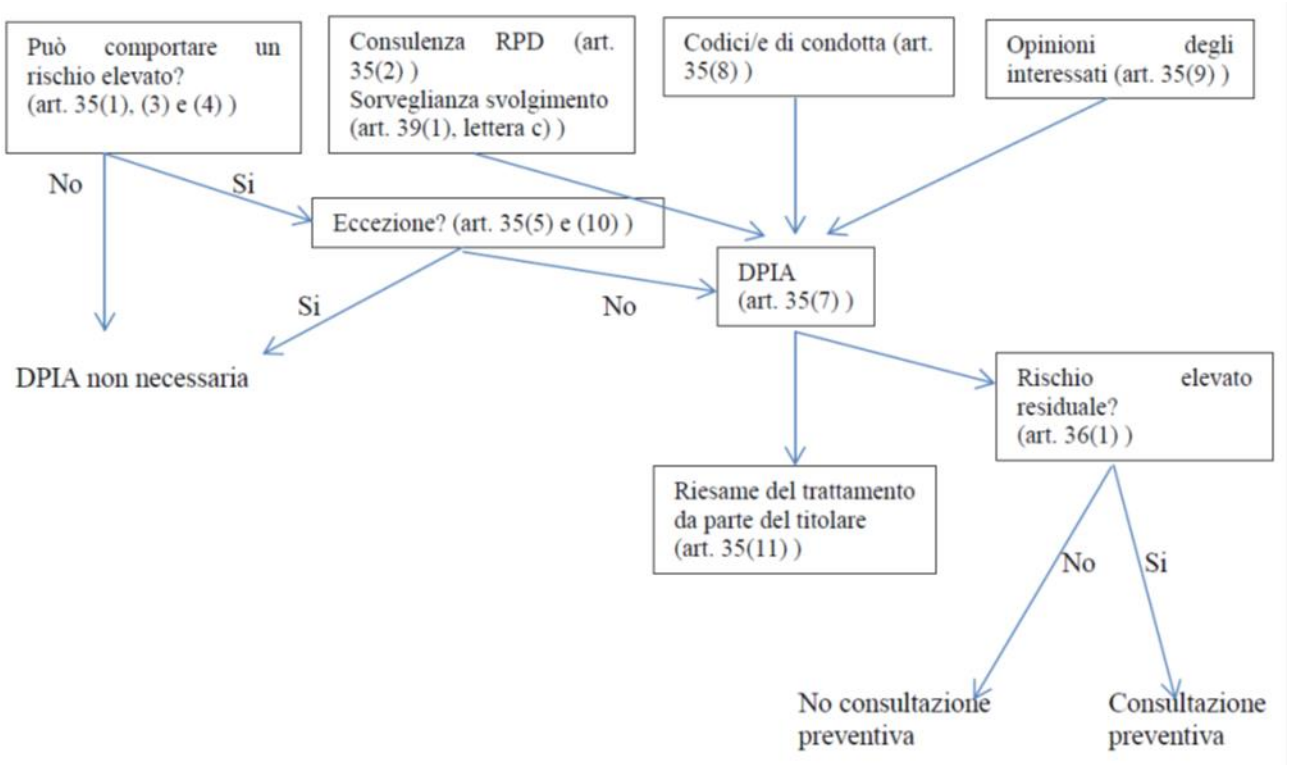
PREMESSA

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA) è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Principi fondanti il processo di DPIA



LA NORMATIVA

A.1. Il Decreto Legislativo 24/2023

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

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

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

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

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

Il RGPD 679/2016

Il trattamento dei dati personali raccolti attraverso i canali di segnalazione interni di cui all'art. 4 del Decreto, comporta l'applicabilità della normativa di protezione contenuta nel **REGOLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 27 aprile 2016**, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati o RGPD).

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

L'**articolo 13, comma 6, del Decreto** prevede che "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d' impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018*".

L'**articolo 35 del RGPD** impone al Titolare di effettuare la DPIA prima di iniziare una data attività di trattamento che possa comportare "*un rischio elevato per i diritti e le libertà delle persone*", in particolare quando prevede di avviare un trattamento mediante "*utilizzo di nuove tecnologie, avuto riguardo alla natura, all'oggetto, al contesto e alle finalità del trattamento*".

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

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

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

Dunque, occorrerà valutare se il trattamento riguardi "*dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza*" o sia finalizzato a valutare aspetti personali "*in particolare mediante l'analisi o la previsione di aspetti riguardanti il rendimento professionale, la*

situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti, al fine di creare o utilizzare profili personali" o se si riferisca a "*dati personali di persone fisiche vulnerabili, in particolare minori*" o se riguardi "*una notevole quantità di dati personali e un vasto numero di interessati*" (v. **Considerando 75 del RGPD**).

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

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

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

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

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

Qualora l'esito della DPIA escluda la sussistenza di un rischio elevato, il Titolare può ritenersi legittimato ad eseguire il trattamento, in caso contrario, non potrà attivare il trattamento senza prima aver adottato le misure idonee a garantire un livello di sicurezza adeguato ai rischi per attenuarli o eliminarli.
Nell'ipotesi residuale in cui il Titolare non sia in grado di individuare dette misure tecniche od organizzative dovrà allora consultare l'Autorità di controllo, ai sensi dell'**articolo 36 del RGPD**, dando luogo alla c.d. consultazione preventiva.

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

ULTERIORI FONTI NORMATIVE

Disposizioni rilevanti in materia sono altresì contenute nei seguenti provvedimenti:

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

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

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI - parere favorevole sullo "Schema di Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali – procedure per la presentazione e gestione delle segnalazioni esterne" predisposto da ANAC. Adottato il 6 luglio 2023;

AUTORITA' NAZIONALE ANTICORRUZIONE (ANAC) - Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone

che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne - Approvate con Delibera n°311 del 12 luglio 2023

METODOLOGIA

I contenuti minimi della DPIA sono specificati come segue all'**articolo 35, paragrafo 7 del RGPD**:

- una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
- le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.
- una valutazione dei rischi per i diritti e le libertà degli interessati;

La metodologia qui adottata per la valutazione di impatto sulla protezione dei dati personali (DPIA), ai sensi dell'art. 35 RGPD, è sviluppata sulla base di quella definita da:

- **Commission nationale de l'informatique et des libertés o CNIL**, l'Autorità francese per la protezione dei dati, in conformità alle Linee guida WP248 e inclusa tra le metodologie raccomandate nell'allegato 1 delle Linee guida stesse;

Al fine di valutare i rischi e le modalità concretamente operative per la corretta protezione dei dati di terze parti, definiti 'interessati', si è proceduto alla valutazione dell'effettivo tipo di dati raccolti e trattati, del modo in cui detti dati vengono raccolti e trattati, dei metodi di conservazione custodia e protezione dei medesimi allo stato della valutazione, il tutto al fine di predisporre idoneo piano di iniziative finalizzate all'adempimento degli obblighi dettati dal citato regolamento per la protezione dei dati, altresì noto come GDPR.

ANALISI DEL CONTESTO

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento riguarda le segnalazioni di illeciti mediante i canali interni istituiti in conformità a quanto previsto dall'articolo 4 del Decreto L.gs 24/2023, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione.

In particolare i canali scelti dal Titolare del Trattamento sono:

- piattaforma informativa fornita da Whistleblowing Solutions Impresa Sociale Srl - incontro diretto con RPCT

Per quanto riguarda la piattaforma informatica Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di Whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

L'architettura di sistema è principalmente composta da:

- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

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.

Quali sono le responsabilità connesse al trattamento?

Titolare del trattamento: UNIONE MUNICIPIA

Responsabile del Trattamento: società Whistleblowing Solution

Sub-responsabili:

Seeweb per gestione infrastruttura IaaS

Trasparency International Italia per la collaborazione nella gestione del Whistleblowing

Titolari autonomi: le amministrazioni deputate ai controlli, Anac, Corte dei Conti, Tribunale

Responsabile della ricezione segnalazione: RPCT

Ci sono standard applicabili al trattamento?

ISO27001

ISO27017

ISO27018

QUALIFICA AGID

CERTIFICAZIONE CSA STAR

Valutazione : Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati identificativi e di contatto dei segnalanti;

Dati identificativi dei segnalati;

Dati di tipo comune contenuti nelle segnalazioni;

Dati particolari contenuti nelle segnalazioni;

Dati relativi a condanne penali e reati contenuti nelle segnalazioni;

Dati identificativi dell'RPCT;

Dati identificativi di eventuale personale a supprto dell'RPCT

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

Piattaforma informatica

È istituita e resa disponibile, quale **canale di segnalazione e di comunicazione con il segnalante, primariamente consigliato**, una piattaforma informatica, raggiungibile via web da chi intenda effettuare una segnalazione, nonché da parte del RPCT e del personale autorizzato.
La piattaforma consente l'acquisizione delle segnalazioni che il segnalante intenda effettuare in forma scritta.

La piattaforma informatica dedicata costituisce un registro speciale di protocollazione e consente l'identificazione di ogni segnalazione ricevuta mediante l'attribuzione di un codice univoco progressivo di 16 caratteri (key code), generato in modo casuale e automatico dalla piattaforma stessa.

Una volta effettuato l'accesso alla piattaforma informatica, il segnalante che non intenda rimanere anonimo, inserisce le informazioni che lo identificano univocamente e le informazioni in suo possesso per identificare eventuali altri soggetti citati nella segnalazione.

La segnalazione inviata mediante piattaforma viene ricevuta su mail dell'Ente indicata dall'RPCT.

Qualora non fosse una mail diretta dell'RPCT, lo stesso provvederà a nominare l'autorizzato alla ricezione di tale mail il cui contenuto, non visibile, sarà immediatamente inviato all'RPCT per la sua apertura mediante credenziali.

Il segnalante che abbia inserito la segnalazione tramite piattaforma non può, successivamente, accedere ad essa attraverso altri canali.

L'utilizzo della piattaforma informatica consente al segnalante di accedere alla propria segnalazione fino a cinque anni successivi alla data dell'archiviazione da parte dell'Amministrazione della segnalazione stessa - tramite l'utilizzo del codice identificativo univoco (key code) che gli viene fornito all'esito della procedura di segnalazione (sia essa anonima o con identificazione) – e di dialogare con l'Amministrazione. Ciò al fine di monitorare lo svolgimento del procedimento amministrativo eventualmente avviato in seguito alla segnalazione.

In ragione delle caratteristiche operative e delle misure tecniche ed organizzative adottate, la medesima piattaforma viene altresì individuata quale strumento gestionale di tutta l'attività (istruttoria compresa) compiuta dal RPCT o suo delegato, in relazione alle segnalazioni pervenute, anche se provenienti da canali differenti.

La piattaforma registra le operazioni svolte dal RPCT e dal personale autorizzato, ai fini dell'attribuzione delle responsabilità delle operazioni eseguite.

Riepilogando il ciclo di vita del trattamento, le fasi sono le seguenti:

-attivazione piattaforma

-configurazione della stessa

-fase d'uso della piattaforma da parte del segnalante per il caricamento delle segnalazioni

-fase d'uso da parte dell'RPCT per la gestione delle segnalazioni

-fase di eventuali comunicazioni ai soggetti da coinvolgere nella gestione della segnalazione

-fase di conservazione dei dati al termine della gestione della segnalazione

<u>Appuntamento con RPCT</u>

Il segnalante che non intenda avvalersi dei canali di segnalazione di cui sopra, può, con qualsiasi mezzo, analogico o digitale, scritto od orale, **chiedere un incontro diretto** che sarà tenuto entro 30 giorni dalla richiesta, dal RPCT o suo delegato.

La richiesta di appuntamento non costituisce segnalazione e non sono raccolte informazioni diverse ed ulteriori rispetto a quelle necessarie alla fissazione e gestione dell'incontro. In particolare, è onere del segnalante non rivelare la propria identità e l'oggetto della segnalazione.

Il personale addetto comunicherà al segnalante il giorno di disponibilità del RPCT per permettere il realizzarsi dell'appuntamento, telefonico od in presenza.

La documentazione e verbalizzazione della segnalazione orale, resa durante l'incontro, avviene nel rispetto di quanto previsto dall'art. 14 del D.Lgs. 24/2023. In particolare, la segnalazione, previo consenso della persona segnalante, è documentata mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione. La verbalizzazione dell'incontro, unitamente alla documentazione analogica eventualmente consegnata dal segnalante è acquisita in modalità digitale, sotto la responsabilità del RPCT, il quale assicura che la conservazione analogica avverrà con modalità tali da proteggere l'identità del segnalante e delle altre persone fisiche che beneficiano della medesima tutela.

Riepilogando il ciclo di vita del trattamento, le fasi sono le seguenti:
-ricezione richiesta appuntamento
-comunicazione della richiesta all'RPCT-verbalizzazione della segnalazione resa durante l'incontro;
-eventuale registrazione della segnalazione previo consenso del segnalante;
-gestione da parte dell'RPCT della segnalazione
-fase di eventuali comunicazioni ai soggetti da coinvolgere nella gestione della segnalazione
-fase di conservazione dei dati al termine della gestione della segnalazione
Eventuale ricezione a mezzo posta

L'Ente ha adottato la seguente procedura a garanzia dell'identità del segnalante:
-inserire la segnalazione in una busta, che deve riportare all'esterno la dicitura "Riservata al Responsabile della Prevenzione della Corruzione e Trasparenza" od altra equivalente, in modo da consentire la comprensione del fatto che si tratta di una segnalazione per la quale si intende mantenere riservata la propria identità e beneficiare delle tutele previste nel caso di eventuali ritorsioni subite in ragione della segnalazione, con indirizzo "_____ – Protocollo Generale – _____";

- -nel caso il segnalante intenda rivelare la propria identità, inserire nella stessa busta un'altra busta chiusa, che deve recare al suo interno un biglietto con indicate le generalità del segnalante (nome, cognome, indirizzo, sede di lavoro, numero di telefono, indirizzo e-mail o pec);
- -nel caso il segnalante non intenda rivelare la propria identità, indicare eventuali modalità con le quali il ricevente potrà comunicare con il segnalante stesso.

Il soggetto ricevente curerà la trasmissione della busta al RPCT, senza aprirla.

La documentazione analogica fatta pervenire dal segnalante è acquisita in modalità digitale per essere conservata sotto la responsabilità del RPCT, il quale assicura che la conservazione analogica avverrà con modalità tali da proteggere l'identità del segnalante e delle altre persone fisiche che beneficiano della medesima tutela.

Eventuali documenti informatici sono registrati nella piattaforma dedicata ed i supporti, utilizzati per la relativa trasmissione, sono conservati con le stesse modalità della documentazione analogica.

La segnalazione dovrà avere i seguenti contenuti:

- tipologia del segnalante (specificare il tipo di rapporto esistente con la Pubblica Amministrazione)
- mansione svolta all'epoca dei fatti segnalati
- autore o autori del fatto e articolazione di appartenenza
- data o periodo in cui si è verificato il fatto. Se possibile indicare anche gli orari
- luogo fisico ove si è svolto il fatto (se il fatto si è svolto in ufficio precisare la denominazione e l'indirizzo della struttura, se il fatto si è svolto fuori dall'ufficio precisare il luogo e l'indirizzo)
-Tipologia di condotta illecita Illeciti penali, amministrativi, civili e contabili:
    - Illeciti commessi in violazione della normativa UE
    - Atti od omissioni che ledono gli interessi finanziari dell'Unione Europea
    - Atti od omissioni riguardanti il mercato interno, che compromettono la libera delle merci, delle persone, dei servizi e dei capitali (art. 26, paragrafo 2, del TFUE)
    - Atti o comportamenti che vanificano l'oggetto o la finalità delle disposizioni dell'Unione Europea
    - Altro
- altre persone interessate (dirigenti, funzionari dell'Amministrazione, privati, imprese) eventuali testimoni dell'episodio
- eventuali altri soggetti ai quali si applicano le misure di protezione, ai sensi del D.Lgs. n. 24 del 2023

È escluso l'utilizzo della posta elettronica quale canale di segnalazione interna.

Quali sono le risorse di supporto ai dati?

Sofware professionale GlobaLeaks;

Infrastruttura IaaS e SaaS privata basata sulle seguenti tecnologie:

-dettaglio Hardware

-VMWARE (virtualizzazione)

-Debian Linux LTS (sistema operativo)

-VEEAM (backup)

-OPNSENSE (firewall)

-OPENVPN (vpn)

Valutazione : Accettabile

ANALISI PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono esplicite, specifiche e legittime.

Sono **esplicite** in quanto sono individuate all'interno del Decreto Legislativo 24/2023 e sono indicate con chiarezza nelle informazioni rese all'interessato ai sensi degli **articoli 13 e 14 del RGPD**;

sono **specifiche** in quanto si riferiscono a tutti i canali di segnalazione interni istituiti dal Titolare;

sono **legittime** in quanto trovano adeguato fondamento nelle disposizioni contenute negli **articoli 6, 9 e 10 del RGPD**.

Il Titolare ha adottato un proprio modello organizzativo per la gestione delle segnalazioni Whistleblowing.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Per il trattamento dei dati personali di tipo comune, le basi giuridiche sono:

- l'interesse pubblico - articolo 6, par. 1, lett e) del GDPR 679/2016
- il consenso (per registrazione) - articolo 6, par. 1, lett a) del GDPR 679/2016

Per il trattamento dei dati particolari, le basi giuridiche sono:

- l'interesse pubblico rilevante - articolo 9, par. 2, lettera g) del GDPR 679/2016
- il consenso (per registrazione) - articolo 9, par. 2, lett a) del GDPR 679/2016

Per il trattamento dei dati giudiziari, le basi giuridiche sono:

- controllo Autorità Pubblica
- autorizzato dal diritto dell'Unione o Stati membri

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)?

I dati raccolti sono solo quelli necessari e pertinenti per la finalità dichiarata.
Per quanto riguarda la piattaforma informatica, la registrazione e attivazione del servizio richiedono solo nome, cognome, ruolo email e telefono dell'utente che effettua la registrazione.
Il software raccoglie segnalazioni secondo i migliori questionari predisposti in ambito

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 ad esempio indirizzi IP, User Agents e altri Metadata.
L'applicativo GlobaLeaks vede abilitata la possiblità di navigazione tamite Tor Browser per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
La piattaforma informatica è configurata in modalità "Custode dell'identità" con limitazione dell'accesso ai dati identificativi del segnalante.
Per quanto riguarda la segnalazione effettuata durante l'incontro con l'RPCT, il modello organizzativo dell'Ente precisa che, sin dalla fase di richiesta appuntamento, non sono raccolte informazioni diverse ed ulteriori rispetto a quelle necessarie alla fissazione e gestione dell'incontro.
Non è consentito effettuare una segnalazione direttamente utilizzando il tradizionale sistema telefonico. Nessun ufficio è autorizzato a ricevere (e gestire) segnalazioni telefoniche.
La documentazione e verbalizzazione della segnalazione orale, resa durante l'incontro, avviene nel rispetto di quanto previsto dall'art. 14 del D.Lgs. 24/2023. In particolare, la segnalazione, previo consenso della persona segnalante, è documentata mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.
La verbalizzazione dell'incontro, unitamente alla documentazione analogica eventualmente consegnata dal segnalante è acquisita in modalità digitale, sotto la responsabilità del RPCT, il quale assicura che la conservazione analogica avverrà con modalità tali da proteggere l'identità del segnalante e delle altre persone fisiche che beneficiano della medesima tutela.
Il modello organizzativo adottato precisa inoltre quale contenuto devono avere le segnalazioni.
In particolare si precisa che le stesse devono contenere:
le circostanze di tempo e di luogo in cui si è verificato il fatto oggetto della segnalazione;
- la descrizione del fatto;
- le generalità o altri elementi che consentano di identificare il soggetto cui attribuire i fatti segnalati.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

Gli utenti che si sono registrati attraverso l'accesso alla propria area riservata possono controllare e aggiornare i loro dati caricati.

Se la segnalazione è verbale, il segnalante può controllare e rettificare quanto emerso nel verbale.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

Sulla piattaforma i dati vengono conservati per 18 mesi prorogabili su richiesta dell'ente ricevente per altri 18 mesi, con cancellazione automatica di quelle scadute.

Da parte del titolare 5 anni dalla comunicazione di chiusura del procedimento avviato a seguito della segnalazione.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati sono informati mediante informativa pubblicata sul sito internet del Titolare del Trattamento.

Inoltre il Titolare ha attivato dei canali interni di segnalazione per portare a conoscenza di tutti i possibili segnalanti la possibilità di avvalersi di tale istituto.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso è richiesto per iscritto per documentare la segnalazione mediante registrazione su un dispositivo idoneo alla conservazione e all'ascolto oppure mediante verbale. In caso di verbale, la persona segnalante può verificare, rettificare e confermare il verbale dell'incontro mediante la propria sottoscrizione.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

Non applicabile

Valutazione : Accettabile

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

La piattaforma consente al segnalante di poter rettificare i suoi dati nella sezione riservata mediante codice univoco a 16 cifre.
Durante l'incontro con l'RPCT la verbalizzazione è oggetto di controllo da parte del segnalante che può procedere a rettifica.
Il contenuto delle segnalazioni effettuate in modalità analogiche è verificabile ed aggiornabile dal segnalante mediante richiesta al Titolare
il diritto di cancellazione non consentito durante il procedimento di gestione della segnalazione. La stessa avviene al termine del periodo di conservazione.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

La piattaforma informatica:
- consente al segnalante la scelta se procedere alla segnalazione in forma anonima o nominativa
- è configurata in modo da non consentire il tracciamento degli utenti che vi accedano dall'interno della rete aziendale
- è configurata per non registrare gli indirizzi IP di navigazione e User agent
non lascia tracce nella cache del browser
- è configurata per consentire l'accesso del segnalante alle proprie segnalazioni, senza necessità di effettuare un'autenticazione (mediante inserimento del solo Codice Univoco)

In caso di consegna della segnalazione con modalità analogiche è prevista l'archiviazione su piattaforma o protocollazione riservata.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

Valutazione : Accettabile

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

Il Titolare ha proceduto a contrattualizzare il responsabile esterno Whistleblowing Solutions I.S. Srl in relazione alle operazioni di trattamento dati personali posti in essere ai soli fini dell'esecuzione del Contratto di servizi (che si allega alla presente DPIA).
Il Responsabile ha altresì inviato i contratti stipulati con i sub responsabili:
-Seeweb per l'attività di archiviazione hosting cloud IASS
-Transparency International Italia per l'attività di supporto utenti e amministratore di sistema

Valutazione : Accettabile

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

Non esiste trasferimento di dati al di fuori dell'Unione Europea

Valutazione : Accettabile

MISURE ESISTENTI O PIANIFICATE

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

Valutazione : Accettabile

Controllo degli accessi logici

L'accesso all'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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Per quanto riguarda l'archiviazione di documentazione raccolta durante o l'incontro con l'RPCT previsto da procedura o ricevuta a mezzo posta, la stessa avviene a cura dell'RPCT in armadi chiusi. La documentazione può essere altresì salvata in piattaforma.

Valutazione : Accettabile

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*

Valutazione : Accettabile

Backup

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

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

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

il Titolare ha adottato una sua procedura di data breach

Valutazione : Accettabile

Lotta contro il 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.

Valutazione : Accettabile

Minimizzazione dei dati

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).

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.

Se la segnalazione avviene a mezzo posta, la procedura indica quali dati inserire in modo da limitare la raccolta di dati eccedenti la finalità.

In caso di segnalazione effettuate a seguito di colloquio richiesto dinnanzi all'RPCT, lo stesso è formato sulla corretta raccolta di dati.

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Il contratto stipulato con il responsabile è stato redatto secondo le Linee Guida Europee e descrive puntualmente il perimetro dei trattamenti affidati al responsabile, le misure di sicurezza e i sub responsabili individuati. Per questi ultimi, il responsabile ha fornito copia dei contratti stipulati nel rispetto delle Linee Guida citate.

Valutazione : Migliorabile

Piano d'azione / misure correttive :

Considerato il potere contrattuale del responsabile scelto per la fornitura della piattaforma, il titolare valuterà eventuali integrazioni richieste ad hoc

Commento di valutazione :

Si ritiene che la parte relativa all'assistenza offerta dal responsabile del servizio possa essere migliorata passando da quella attuale ad una assistenza più professionale

Gestione delle politiche di tutela della privacy

Il Titolare del Trattamento ha nominato un Responsabile per la Protezione dei Dati.

Il Titolare del Trattamento ha nominato gli autorizzati al trattamento e contrattualizzato il responsabile.

Ha inoltre visionato e conservato tutta la documentazione relativa alla compliance al G.D.P.R. 679/2016 del responsabile, comprese le certificazioni possedute.

L'Ente ha aggiornato il registro dei trattamenti inserendo il trattamento Whisleblowing.

L'Ente ha da tempo adottato la procedura per la gestione del data breach.

Valutazione : Accettabile

Gestione dei rischi

Tutto il personale dell'Ente è stato formato in materia di protezione dati personali.

Sono stati mappati tutti i trattamenti nel registro.

Valutazione : Accettabile

Gestione del personale

Viene effettuata adeguata formazione per la corretta sensibilizzazione.

Vengono effettuate sedute di formazione specifiche in base all'evolversi della normativa.

Valutazione : Accettabile

ESECUZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI (DPIA)

Il trattamento dei dati personali è un'attività che espone a rischio gli interessati, ossia le persone fisiche cui i dati si riferiscono.
I rischi per i diritti e le libertà delle persone fisiche possono derivare dal fatto che il trattamento, in ragione delle caratteristiche sue proprie, possa cagionare danni materiali e immateriali, come per esempio, discriminazioni, pregiudizio alla reputazione o qualsiasi altro danno economico o sociale significativo (**Considerando 75 del RGPD**).

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

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

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

ANALISI DEI POSSIBILI IMPATTI E LORO GRAVITÀ

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

Scala di misurazione dell'impatto (suggerita da ENISA)

LIVELLO DI IMPATTO	DESCRIZIONE
BASSO	Gli individui possono andare incontro a disagi minori, che supereranno senza alcun problema (tempo trascorso reinserendo informazioni, fastidi, irritazioni, ecc.)
MEDIO	Gli individui possono andare incontro a significativi disagi, che saranno in grado di superare nonostante alcune difficoltà (costi aggiuntivi, rifiuto di accesso ai servizi aziendali, paura, mancanza di comprensione, stress, disturbi fisici di lieve entità, ecc.)
ALTO	Gli individui possono andare incontro a conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento in liste nere da parte di istituti finanziari, danni alla proprietà, perdita di posti di lavoro, citazione in giudizio, peggioramento della salute, ecc.)
MOLTO ALTO	Gli individui possono subire conseguenze significative, o addirittura irreversibili, che non sono in grado di superare (incapacità di lavorare, disturbi psicologici o fisici a lungo termine, morte, ecc.)

ANALISI DELLE MINACCE

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

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

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

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

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

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

Tradizionalmente si individuano le seguenti **tipologie di accadimento**, dalle quali si possono originare delle fonti di rischio.

Le fonti di rischio possono essere rappresentate da:

- **persona, interna o esterna all'ente**, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, ...);
- **fonte non umana** (acqua, fuoco, eventi naturali, materiali pericolosi, virus informatici, ecc.) che può essere all'origine di un rischio. Può essere un incidente od un sinistro verificatosi presso uno dei soggetti incaricati del trattamento od anche presso Contitolari e Responsabili del trattamento

Possono costituire una "**fonte di rischio umana interna**" le seguenti situazioni:

- un dipendente malintenzionato che usa la sua vicinanza al sistema, le sue competenze, i suoi privilegi e un tempo a disposizione potenzialmente considerevole, ovvero un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione.
- un utente o il suo entourage, negligente o malintenzionato, che ha accesso al servizio.

Le motivazioni possono essere molteplici: confusione, errore, negligenza, vendetta, volontà di provocare allarme, malevolenza, possibilità di lucro, spionaggio.

Possono costituire una "**fonte di rischio umana esterna**" le seguenti situazioni:

- una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio;
- un attaccante che prende di mira un utente sfruttando la sua conoscenza dell'utente e alcune informazioni su quest'ultimo;
- un attaccante che prende di mira una delle società incaricate del trattamento sfruttando la sua conoscenza di tali società, così da consentirgli di minarne l'immagine;
- una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

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

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

ANALISI DELLA PROBABILITÀ DI VERIFICAZIONE

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

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

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

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

ANALISI DEL RISCHIO

Il seguente schema rappresenta una griglia oggettiva di calcolo delle Probabilità e Gravità con riguardo ai diritti e libertà dell'interessato.

Matrice di rischio: RI=P*G					
	Probabilità	1 – trascurabile	2 – limitata	3 – importante	4 - massima
Gravità	1- trascurabile	1	2	3	4
	2 – limitata	2	4	6	8
	3 – Importante	3	6	9	12
	4 - Massima	4	8	12	16

Valutazione % delle misure esistenti

Rating	**Descrizione**	
1-25%	Non adeguate	Il controllo non è previsto o è assente nella pratica.
26-50%	Parzialmente adeguate	Il controllo è applicato sporadicamente o in modo inadeguato, non garantendone quindi l'efficacia
51-57%	Quasi adeguate	Sono state rilevate mancanze, soprattutto di tipo formale (per esempio, inesattezze nelle procedure).
58-100%	Adeguate	Il controllo è sistematicamente applicato e non sono state rilevate inadeguatezze al controllo.

Elementi per la valutazione:

Ri è il Rischio Inerente valore di riferimento su cui effettuare le valutazioni e le operazioni di mitigazione.

Rr è il Rischio Residuo calcolato al netto delle misure di mitigazione del rischio (determinate in via percentuale - % abbattimento).

L'azienda valuta come Rischio Accettabile (Ra) = 3

Se il rischio inerente Ri a seguito delle valutazioni oggettive, dovesse risultare superiore ad Ra, l'azienda interverrà con mitigazioni opportune tali che ad Rr < Ra

VALUTAZIONE

Rischio - Accesso illegittimo ai dati

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

Perdita di riservatezza, perdita del posto di lavoro, perdite economiche, danni psicologici, diffamazione

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso illegittimo alle credenziali per decrittografare, accesso ai luoghi fisici di conservazione, divulgazione verbale dei fatti segnalati, divulgazione verbale dei soggetti segnalati e segnalanti

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Archiviazione, Backup, Manutenzione, Vulnerabilità, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro il malware, Sicurezza dei canali informatici, Minimizzazione dei dati, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Gestione del personale, Tracciabilità

Calcolo del rischio

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

Valutazione : Accettabile

Rischio - Modifiche indesiderate dei dati

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

danni psicologici, perdita del posto di lavoro, diffamazione, perdite economiche

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

accesso ai luoghi fisici di conservazione, accesso illegittimo alle credenziali per decrittografare

Quali sono le fonti di rischio?

Fonti non umane, Fonti umane esterne, Fonti umane interne

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

Crittografia, Archiviazione, Backup, Manutenzione, Sicurezza dei canali informatici, Vulnerabilità, Controllo degli accessi logici, Tracciabilità, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro il malware, Minimizzazione dei dati, Contratto con il responsabile del trattamento, Gestione delle politiche di tutela della privacy, Gestione dei rischi, Gestione del personale

Calcolo del rischio

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

Valutazione : Accettabile

Rischio - Perdita di dati

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

perdita del posto di lavoro se associata a perdita di riservatezza, perdite economiche, mancato seguito alla segnalazione, perdita di fiducia nelle istituzioni pubbliche

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

accesso ai luoghi fisici di conservazione, accesso illegittimo alle credenziali per decrittografare

Quali sono le fonti di rischio?

Fonti non umane, Fonti umane esterne, Fonti umane interne

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

Controllo degli accessi logici, Archiviazione, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestione dei rischi

Calcolo del rischio

G	P	Ri	Mitigazione % abbattimento rischio	Rr
3	2	6	70%	1,8

Valutazione : Accettabile

VALUTAZIONI E PIANO DI TRATTAMENTO DEI RISCHI

Premesso che:

- a norma dell'**articolo 35, paragrafo 9, del RGPD** "*Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti*";
- a norma dell'**articolo 36, paragrafo 1, del RGPD** "*Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio*";
- con particolare riferimento alla c.d. **consultazione preventiva** di cui all'art. 36 del RGPD, si recepiscono le indicazioni contenute nelle Linee Guida rilasciate dal Gruppo di lavoro articolo 29 per la protezione dei dati, come modificate e adottate da ultimo il 4 ottobre 2017 (**WP 248 rev.01**), a tenore delle quali "*Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo*". "*Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5)*"

Si stabilisce quanto segue:

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati

aventi l'obbligo di DPIA, emergono "Rischi inerenti (Ri)" con impatto sui diritti e libertà degli interessati con stima a Valore Medio.

Nell'ottica di mitigazione di tali rischi, si evince che, con l'implementazione delle misure tecnico/organizzative pianificate ad integrazione di quelle messe in atto, il valore di rischio residuo rientra nei parametri accettabili uguali o minori rispetto al "Rischio accettato (Ra)" dall'organizzazione aventi stima a Valore basso, valore ritenuto accettabile dall'organizzazione in relazione dai parametri oggettivi considerati.

Si ritiene pertanto che il trattamento in oggetto presenta un grado di rischio sui diritti e le libertà dell'interessato rientrante nei parametri accettabili e di conseguenza non è richiesta una

consultazione preventiva all'Autorità Garante.

PARERE DEGLI INTERESSATI

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

PARERE DPO

DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

ACQUISITO IL PARERE DEL RESPONSABILE DELLA PROTEZIONE DEI DATI PERSONALI (RPD)

Alla luce delle informazioni raccolte e dei risultati della presente valutazione di impatto, **SI RITIENE** possibile procedere con l'attivazione dei canali di segnalazione interni e l'avvio del trattamento senza ulteriori misure tecniche e organizzative.

FORMALIZZAZIONE DEI RISULTATI, REVISIONE ED AGGIORNAMENTO

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

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

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

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

DATA……..

FIRMA

TITOLARE DEL TRATTAMENTO

INFORMATIVA AI SENSI DEGLI ART. 13 - 14 DEL GDPR 2016/679
WHISTLEBLOWING - SOGGETTI CHE SEGNALANO ILLECITI D.LGS 24/2023

I dati personali sono trattati da UNIONE MUNICIPIA nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità dell'Ente, dai soggetti che, in ragione del proprio rapporto di lavoro presso l'Ente, vengano a conoscenza di condotte illecite, in particolare:

a) Dipendenti;
b) Lavoratori autonomi che svolgono la propria attività lavorativa presso i soggetti del settore pubblico;
c) Liberi professionisti e consulenti;
d) Volontari e tirocinanti, retribuiti e non retribuiti, che prestano la propria attività presso
e) soggetti del settore pubblico;
f) Persone con funzioni di amministrazione, direzione, controllo, vigilanza o rappresentanza, anche qualora tali funzioni siano esercitate in via di mero fatto, presso soggetti del settore pubblico;

Oggetto di segnalazione sono le informazioni sulle violazioni, compresi i fondati sospetti, di normative nazionali e dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato **commesse nell'ambito dell'organizzazione dell'ente** con cui il segnalante o denunciante intrattiene uno di rapporti giuridici qualificati considerati dal legislatore

Tipi di dati trattati e finalità del trattamento

I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza in ragione del proprio rapporto di servizio con l'Ente commesse dai soggetti che a vario titolo interagiscono con il medesimo, vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti.

La base giuridica è rappresentata;

dall'interesse pubblico e dall'interesse alla integrità dell'amministrazione pubblica;

dal consenso per la registrazione su un dispositivo idoneo alla conservazione e all'ascolto in caso di incontro diretto con l'RPCT.

I dati trattati sono:

Dati comuni di tipo anagrafico dei soggetti segnalati

Eventuali dati particolari e giudiziari dei segnalati

Dati dei segnalanti necessari alla gestione della segnalazione

La gestione e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati.

Modalità di trattamento

Digitale e analogica

Comunicazione dei dati

Qualora, all'esito della verifica, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, il RPCT provvederà a trasmettere l'esito dell'accertamento per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:

a) al Responsabile dell'Area Risorse Umane, nonché al Responsabile dell'unità organizzativa di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare;
b) agli organi e alle strutture competenti dell'Ente affinché adottino gli eventuali ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;
c) se del caso, all'Autorità Giudiziaria, alla Corte dei conti e all'ANAC. In tali eventualità nell'ambito del procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale; nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa. Qualora la contestazione sia fondata, in tutto o in parte, sulla segnalazione e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità

Whistleblowing Solutions Impresa Sociale S.r.l. quale fornitore del servizio di erogazione e gestione operativa della piattaforma tecnologica di digital whistleblowing gestisce i dati in qualità di Responsabile del trattamento ai sensi dell'art. 28 del Regolamento UE 2016/679.

Periodo di conservazione

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 e per un massimo di anni 5.

Diffusione

I dati non sono oggetto di diffusione.

Diritti degli interessati

Rispetto alla specifica disciplina del D. Lgs. n. 24/2023, occorre tenere in considerazione le limitazioni di cui all'art. 2-undecies del D. Lgs. n. 196/2003 all'esercizio dei diritti sanciti dagli articoli da 15 a 22 del Re-golamento (UE) 2016/679.

Dall'esercizio di tali diritti potrebbe derivare un pregiudizio effettivo e concreto alla tutela della riservatezza dell'identità della persona segnalante.

In tali casi, dunque, la persona coinvolta o la persona menzionata nella segnalazione, con riferimento ai propri dati personali trattati nell'ambito della segnalazione, non possono esercitare – **per il tempo e nei limiti in cui ciò costituisca una misura necessaria e proporzionata** - i diritti che normalmente il Regolamento (UE) 2016/679 riconosce agli interessati (il diritto di accesso ai dati personali, il diritto a rettificarli, il diritto di ottenerne la cancellazione o cosiddetto diritto all'oblio, il diritto alla limitazione del trattamento, il diritto alla portabilità dei dati personali e quello di opposizione al trattamento).

In tali casi, dunque, al soggetto segnalato o alla persona menzionata segnalazione è preclusa anche la possibilità, laddove ritengano che il trattamento che li riguarda violi suddetti diritti, di rivolgersi al titolare del trattamento e, in assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della protezione dei dati personali.

In tutti gli altri casi è garantito l'esercizio dei diritti sopra citati.

Dati di contatto

L'interessato potrà rivolgere le sue richieste o esercitare i suoi diritti rivolgendosi ai seguenti contatti:

Titolare	UNIONE MUNICIPIA	Tel. 0375/969021 Mail: sindaco.motta@unionemunicipia.it Pec: unione.mottab.scandolarar@pec.regione.lombardia.it
DPO	Dott.ssa Simona Persi	
Responsabile della prevenzione della corruzione e della trasparenza	Dr.ssa Maria Rita Nanni	sindaco.motta@unionemunicipia.it

Motta Baluffi, 16/02/2024

Il Titolare

UNIONE MUNICIPIA

IL PRESIDENTE : ENNIO ROBERTO OLIVA