COMUNE DI TERDOBBIATE

PROVINCIA DI NOVARA

WHISTLEBLOWING

DECRETO LEGISLATIVO 10 marzo 2023, n. 24
Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

DATA PROTECTION IMPACT ASSESSMENT

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(art.35 Regolamento UE/2016/679 GDPR)

Sommario

PARTE I-Premessa

La presente valutazione d'impatto è stata svolta e redatta dal Responsabile della prevenzione della corruzione e della trasparenza del Comune di Terdobbiate, Dott.ssa Giuliana Balbo.

Normativa di riferimento

Ai fini della redazione del presente atto di fa riferimento specificatamente ai seguenti atti normativi:

- 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);
- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal Decreto Legislativo 10 agosto 2018 n.101;
- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) [Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679 Versione adottata l'11 aprile 2018];
- Decreto Legislativo 18 agosto 2000, n. 267. Testo unico delle leggi sull'ordinamento degli enti locali.
- Legge 30 Novembre 2017, n. 179 “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.”
- Legge 6 Novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione.”
- Decreto Legislativo 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.”

PARTE II-INQUADRAMENTO DELLA DPIA

Lo scopo della valutazione d’impatto o DPIA

La valutazione d’impatto è una procedura, nota anche con l’acronimo DPIA (Data Protection Impact Assessment) o PIA (Privacy Impact Assessment), come si indicherà nel seguito, ed è prevista dall’articolo 35 del Regolamento UE/2016/679 (GDPR) e ha lo scopo di descrivere un trattamento di dati per valutarne la necessità e la proporzionalità così come tutti gli altri principi fondamentali del GDPR.
Il processo di PIA può riguardare un singolo trattamento anche più trattamenti che presentino analogie per natura, ambito, finalità e rischi.
Dalla descrizione del trattamento ne consegue la valutazione e quindi la predisposizione di idonee misure per affrontarlo.

La PIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare a rispettare le prescrizioni normative ma attesta anche di aver adottato idonee misure per garantirne il rispetto.

Obbligo della PIA

1. L'OBBLIGO SECONDO LE PRESCRIZIONI DEL DGPR.

Il PIA (Privacy Impact Assessment) è obbligatorio in tutti i casi previsti dall'articolo 35 comma 1 del Reg.UE 2016/679 DGPR ossia quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e questo può avvenire per varie ragioni:

- per l'implementazione di nuove tecnologie;
- a causa della natura, dell'oggetto, del contesto o delle finalità del trattamento.

Lo stesso articolo 35 del Reg.UE 2016/679 DGPR al comma 3 cita anche alcune ipotesi specifiche che rendono sempre obbligatoria la PIA che sono:

- la valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche (art.35 c.3 p.a GDPR)
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10 (art.35 c.3 p.b GDPR);

2 GLI ULTERIORI OBBLIGHI DI PIA INTRODOTTI DAL GARANTE PER LA PRIVACY.

Il GDPR ha previsto espressamente che l'autorità nazionale di controllo ha il potere e la facoltà di prevedere delle specifiche tipologie di trattamento per i quali è obbligatoria l'adozione del PIA (art.35 c.4 GDPR), in questi casi ha l'obbligo di pubblicare il provvedimento e comunicarlo al comitato europeo per la protezione dei dati (art.35 c.6 GDPR) che era Gruppo di lavoro art.29 o Working Party article 29 (noto anche con l'acronimo WP29), fino al 25 maggio del 2018 (data di entrata in vigore del RGPD) e aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali, ed è stato sostituito in seguito dal Comitato europeo per la protezione dei dati (art.68 GDPR).

Per specificare nel dettaglio e dare maggiore certezza è intervenuto il provvedimento del Garante per la Protezione dei Dati Personali che con la delibera 11 ottobre 2018, n.467 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679*", che ha attuato le indicazioni del Working Party article 29 del 2017 fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

In questo modo si è stabilito l'obbligo di PIA nei casi in cui ricorrano almeno due di questi criteri anche se il titolare può deciderla anche quando ne ricorra uno solo in funzione delle implicazioni sulla sicurezza:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es. videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es. informazioni sulle opinioni politiche);
- trattamento di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per differenti finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene ad esempio con i big data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, devices Internet of Things, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

Il decreto legislativo 10 marzo 2023 n. 24 di recepimento della direttiva Ue 2019/1937 sulla segnalazione di illeciti per contrastare fenomeni corruttivi, sia nelle imprese private sia nelle pubbliche amministrazioni prevede all'articolo 13, dedicato al trattamento di dati personali nei procedimenti di whistleblowing, al comma 6 che gli enti debbano definire 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".

Chi deve svolgere la PIA

Il titolare del trattamento ha la responsabilità di valutare la necessità del Privacy Impact Assessment (art.35 c.2 DGPR) e, laddove si renda necessaria, l'obbligo di provvedere alla realizzazione sovrintendendo sempre ogni fase pur se la realizzazione materia sia demandata ad altro soggetto (consulente esterno o dipendente).
Nella decisione sulla realizzazione e nello svolgimento si consulta con il DPO/RDP (Data protection officer/Responsabile per la protezione dei dati) inoltre, se il trattamento lo richiede, può acquisire pareri di esperti, tecnici e in particolare del responsabile della sicurezza dei sistemi informativi (noto anche come Chief Information Security Officer, acronimo CISO) e del responsabile IT (acronimo di Information Technology), laddove presenti, da allegare alla PIA.
Se lo ritiene necessario, il titolare può acquisire anche il parere degli interessati o dei loro rappresentanti purché ciò non pregiudichi gli interessi pubblici dell'ente che procede e purché non si mettano a rischio i trattamenti stessi che si vogliono valutare con la PIA (art.35 c.9 DGPR).

Nel caso oggetto di questa DPIA il titolare del trattamento è tenuto a predisporre la DPIA in adempimento ad un preciso obbligo di legge.

Aggiornamento della PIA

La PIA non è un documento statico ma proprio per le sue finalità generali richiede un processo costante di verifica ed eventuale aggiornamento perlomeno quando insorgono variazioni del rischio, secondo il contesto e le evoluzioni tecnologiche, ovvero mutino o si evolvano le attività relative al trattamento.
In questi casi il titolare del trattamento procede a un riesame per valutare se dalle variazioni delle procedure del trattamento che sono intervenute e/o dalle mutate condizioni del contesto ne scaturisca un pregiudizio, anche solo potenziale, sulla sicurezza del trattamento dei dati personali e se le previsioni contenute nel PIA siano ancora valide e attuali (art.35 c.11 DGPR).

I principi di valutazione del trattamento

La valutazione della PIA deve informarsi ai valori e ai criteri generali del trattamento dei dati contenuti nel GDPR e in particolare verificare che siano attuati i principi di:

- liceità, correttezza e trasparenza (art.5 c.1 p.a GDPR);
- limitazione delle finalità (art.5 c.1 p.b GDPR);
- minimizzazione dei dati (art.5 c.1 p.c GDPR);
- esattezza (art.5 c.1 p.d GDPR);
- diritto all'oblio (art.5 c.1 p.e GDPR);
- integrità e riservatezza (art.5 c.1 p.f GDPR);
- responsabilizzazione (art.5 c.2 GDPR).

1. LICEITÀ, CORRETTEZZA E TRASPARENZA.

L'articolo 5 comma 1 punto a del GDPR impone che i dati personali siano sempre trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Il principio di correttezza va a sostituire il principio di lealtà precipuo della vecchia normativa nella quale dominava un rapporto tra il titolare e l'interessato mentre oggi l'impegno è esteso all'intera società nella quale tutti noi viviamo e esplichiamo i nostri diritti e doveri, per cui il trattamento deve essere corretto, così garantendo all'intera collettività che il trattamento non ponga a rischio i dati personali.
La definizione del principio di correttezza è stata formulata già dal Gruppo di lavoro art.29 o Working Party article 29 (noto anche con l'acronimo WP29), sostituito oggi dall'European Data Protection Board (noto anche con l'acronimo EDPB), che è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati, con riferimento alla chiarezza e trasparenza delle informative, sostenendo la necessità che l'informazione fornita all'interessato debba essere tale da far comprendere in modo adeguato, "le modalità con cui i dati sono raccolti, utilizzati e consultati grazie ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro" (art.12 c.1 GDPR) e anche le conseguenze.
Quindi, il principio di liceità e correttezza è funzionale e rafforzativo dell'obbligo di trasparenza del trattamento nei confronti degli interessati che rappresenta un vero e proprio diritto dell'interessato. Il

punto di partenza della PIA è la valutazione della documentazione complessiva relativa al trattamento dei dati e in particolare dell'informativa resa agli interessati.

2. LIMITAZIONE DELLE FINALITÀ.

L'articolo 5 comma 1 punto b del GDPR stabilisce che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità, quindi secondo un principio generale di necessità e proporzionalità che deve applicarsi a tutte le informazioni relative alle persone fisiche e quindi la valutazione della PIA deve escludere che possano esserci dei trattamenti indiscriminati.
Il titolare del trattamento deve stabilire quindi, prima dell'inizio del trattamento, in maniera precisa e tassativa evitando formulazioni generiche o illimitate, gli scopi in base ai quali ha intenzione di raccogliere e trattare i dati personali e deve limitarsi alle finalità che ha comunicato all'interessato prima dell'inizio della raccolta dei dati e quindi del trattamento.
Ciò implica che se alcuni dei dati personali o se i dati personali di alcuni soggetti non servono per le finalità del trattamento, essi non devono neppure essere raccolti e la PIA deve quindi verificare che ciò non avvenga nel processo dell'intero trattamento.

3. MINIMIZZAZIONE DEI DATI.

Il principio di minimizzazione dei dati parte dall'idea fondamentale che il titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, pertanto l'articolo 5 comma 1 punto c del GDPR impone che i dati personali oggetto di trattamento abbiano le caratteristiche di:

- adeguatezza, vale a dire proporzionalità rispetto alle finalità per la quale sono raccolti;
- pertinenza rispetto alle finalità precedentemente definite;
- limitazione a quanto necessario al raggiungimento delle finalità per i quali sono trattati.

Dunque i dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire, ed essi non possono essere raccolti in misura maggiore a quella necessaria.
In sostanza si stabilisce l'obbligo di verificare che per le esigenze del trattamento siano raccolti e gestiti il minor quantitativo di dati possibili.
La PIA, per questo fine, deve conoscere l'estensione dei trattamenti e valutare l'effettiva necessità dell'estensione della base di dati trattati rispetto alle finalità.

4. ESATTEZZA DEI DATI.

L'articolo 5 comma 1 punto d del GDPR impone che i dati trattati devono essere esatti e, se necessario, aggiornati.
Il titolare, inoltre, deve prendere tutte le misure ragionevoli per cancellare o rettificare tempestivamente quelli che non sono più esatti e, laddove non rilevi errori di sua iniziativa, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, può chiedere anche l'integrazione dei dati personali incompleti fornendo, eventualmente, una dichiarazione integrativa (art.16 GDPR).

La PIA, a questo scopo, deve verificare le misure e i sistemi di verifica sulla correttezza dei dati.

5. DIRITTO ALL'OBLIO.

Il diritto all'oblio, inizialmente riconosciuto soltanto a livello giurisprudenziale sia in campo europeo che nazionale, può essere definito come l'interesse di un singolo ad essere dimenticato e consiste, quindi, nell'obbligo automatico di eliminazione dei trattamenti quando vengono meno la finalità per cui sono trattati, è espressamente riconosciuto dall'articolo 17 del DGPR quando si verifichino le seguenti condizioni:

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati (art.17 c.1 p.a GDPR);
2. l'interessato revoca il consenso su cui si basa il trattamento (art.17 c.1 p.b GDPR);
3. l'interessato si oppone al trattamento nei casi previsti (art.17 c.1 p.c GDPR);
4. i dati personali sono stati trattati illecitamente (art.17 c.1 p.d GDPR);
5. sussiste un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro per cancellare i dati personali (art.17 c.1 p.e GDPR);
6. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione (art.17 c.1 p.f GDPR).

In tutti questi casi il titolare del trattamento è obbligato a cancellare ogni dato, anche quelli resi eventualmente pubblici secondo la tecnologia disponibile, e in questi casi informerà anche gli altri titolari del trattamento che siano in possesso dei dati personali degli interessati che hanno richiesto la cancellazione affinché provvedano a eliminare i propri trattamenti e cancellino qualsiasi link o copia.

L'articolo 5 comma 1 punto e del GDPR impone l'obbligo di eliminare o, nei casi previsti, di rendere anonimi i trattamenti nell'esatto momento in cui essi non sono più giustificati secondo i principi che si sono indicati in precedenza, pertanto il procedimento oggetto della verifica PIA deve valutare che sussista un sistema automatizzato che, prescindendo dalla richiesta dell'interessato e/o dalla revoca del consenso, laddove esso sia il fondamento giuridico del trattamento, elimini il trattamento quando si verifichino queste condizioni.
L'eliminazione può essere sostituita dall'anonimizzazione dei dati per scopi di archiviazione nel pubblico interesse, di ricerca scientifica o storica ovvero a fini statistici.
Il diritto all'oblio è espressamente escluso in casi tassativamente previsti e specificatamente quando il trattamento si rende necessario:

1. per l'esercizio del diritto alla libertà di espressione e di informazione (art.17 c.3 p.a DGPR);
2. per l'adempimento di un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art.17 c.3 p.b DGPR);
3. per motivi di pubblico interesse nella sanità pubblica (art.17 c.3 p.c DGPR);
4. a fini di archiviazione e di statistica nel pubblico interesse, di ricerca scientifica o storica (art.17 c.3 p.d DGPR);
5. in ambito giudiziario per l'esercizio o la difesa di un diritto (art.17 c.3 p.e DGPR).

6. PRINCIPIO DI INTEGRITÀ E RISERVATEZZA.

Il principio di integrità e riservatezza è previsto dall'articolo 5 comma1 punto f del GDPR e stabilisce che i dati devono essere sempre trattati in modo da garantirne una sicurezza adeguata.
Il titolare del trattamento ha l'obbligo quindi di adottare tutte le misure di sicurezza tecniche e organizzative adeguate al fine di proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro sottrazione, perdita, distruzione, danni accidentali, ossia da tutte quelle ipotesi che configurerebbero un data breach (art.34 GDPR).

La PIA quindi deve verificare preventivamente che la sicurezza sia garantita nei confronti dei dati lungo l'intero ciclo del trattamento e, laddove non sia possibile eliminare del tutto il rischio che siano adottate tutte le misure disponibili, sul piano fisico e tecnologico, per minimizzare il rischio.

7. PRINCIPIO DI RESPONSABILITÀ.

Il principio di accountability previsto nel testo originale del GDPR approvato in lingua inglese, previsto dall'articolo 5 comma 2 del GDPR, è stato tradotto come "responsabilizzazione" e definito come l'obbligo posto in capo al titolare del trattamento di essere competente, e quindi concretamente in grado, di garantire i principi generali del trattamento indicati in precedenza e altresì di poterlo comprovare.
Da ciò ne consegue l'obbligo di una gestione aziendale "responsabile" che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale e la responsabilizzazione del titolare del trattamento a cui viene affidato sia il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali in considerazione della realtà produttiva nella quale opera.
La PIA quindi deve valutare anche l'impegno progettuale, nell'ottica del principio di privacy by design, e l'azione concreta del titolare, nell'attuazione del concetto di privacy by default, rispetto l'organizzazione della gestione di tutti i trattamenti svolti.

Contenuti

La PIA deve contenere, oltre la generale e complessiva valutazione dell'impatto del trattamento sulle libertà e sui diritti delle persone fisiche, alcune parti ritenute inderogabilmente essenziali dal DGPR (art.35 c.7 DGPR):

1. DESCRIZIONE GENERALE DEL TRATTAMENTO COMPLESSIVO: contenente la descrizione sistematica del trattamento complessivo e delle singole procedure che lo compongono, delle finalità e, se possibile, l'esplicazione dell'interesse legittimo perseguito dal titolare (art.35 c.7 p.a DGPR).
2. VALUTAZIONE DELLA PROPORZIONALITÀ: di tutti i singoli trattamenti valutati in relazione alle loro finalità (art.35 c.7 p.b DGPR).
3. RISK ANALYSIS: ossia una valutazione dettagliata dei rischi derivanti dal trattamento che possano sui diritti e sulle libertà degli interessati (art.35 c.7 p.c DGPR).
4. IL PROGETTO OPERATIVO: contenente il dettaglio delle misure di sicurezza predisposte per affrontare i rischi sulla sicurezza dei dati personali nella misura più

efficace in modo da poter dimostrare la conformità del trattamento alle precisioni del Regolamento Europeo (art.35 c.7 p.d DGPR).

Esiti finali della PIA

Acclarato che l'obiettivo sostanziale della PIA è quello di rendere più vicino possibile allo zero il rischio di procurare danni alle libertà e ai diritti o all'interessato, essa compie una valutazione puntuale dello stato di fatto ("as is") ponendo la sua attenzione sui rischi legati al trattamento e valutandoli al netto delle attività poste in essere o pianificate per contenerlo e ridimensionarlo sulla base delle valutazioni del titolare del trattamento, del responsabile del trattamento e del DPO.
All'esito dello svolgimento della valutazione d'impatto si possono avere differenti conseguenze:

ELIMINAZIONE O COMPENSAZIONE DEI RISCHI.

Qualora il titolare riesca con il processo di PIA a identificare correttamente e a eliminare o attenuare sufficientemente il rischio, inizia il trattamento dopo aver completato la valutazione d'impatto, con il percorso previsto dal DGPR, rendendo disponibile la PIA agli organi di controllo e a chi ne abbia titolo.

1. SUSSISTENZA RESIDUA DI RISCHI.

Quando all'esito della valutazione d'impatto si ritenga che il trattamento mantenga rischi elevati residuali, il trattamento non può aver luogo e si deve procedere alla preventiva consultazione del Garante, in questo caso il titolare del trattamento deve inviare la PIA all'Autorità di controllo e deve comunicare:

a) LE FINALITÀ E I MEZZI DEL TRATTAMENTO (art.36 c.3 p.b DGPR);
b) I RUOLI DEPUTATI AL TRATTAMENTO: dettagliando le responsabilità del titolare del trattamento, l'eventuale presenza e l'accordo sulla ripartizione del trattamento con contitolari del trattamento, la nomina di responsabili del trattamento, il tutto con particolare attenzione nel caso in cui il trattamento avvenga nell'ambito di un gruppo imprenditoriale (art.36 c.3 p.a DGPR);
c) LE MISURE DI SICUREZZA: che sono state previste per proteggere i diritti e le libertà degli interessati e per rendere quindi il trattamento conforme al regolamento (art.36 c.3 p.c DGPR);
d) I DATI E I RECAPITI DEL DPO (art.36 c.3 p.d DGPR);
e) OGNI ALTRA INFORMAZIONE UTILE: che sia richiesta dall'autorità di controllo (art.36 c.3 p.f DGPR).

Se il Garante ritenga che il trattamento violi il DGPR poiché il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce un parere scritto, entro otto settimane dalla richiesta di consultazione al titolare del trattamento e, se presente, al responsabile del trattamento, il termine può essere ulteriormente prorogato di sei settimane nei casi di trattamenti particolarmente complessi, previo avviso.

PARTE III-METODOLOGIA DI ESECUZIONE DELLA DPIA

Premessa metodologica

La PIA (Privacy Impact Assessment) è un processo codificato e strutturato in fasi, dunque uno strumento operativo, che aiuta le organizzazioni aziendali ad analizzare con sistematicità, ad individuare e a ridurre i rischi privacy per gli individui interessati coinvolti dal rilascio di un nuovo progetto, soluzione o regola.
La valutazione d'impatto del trattamento dei dati personali costituisce parte integrante dell'approccio Privacy by Design, ed aiuta ad assicurare che i problemi potenziali siano identificati negli stadi iniziali del progetto quando la possibilità di indirizzarli è spesso più efficace e meno costosa.
Le sue fasi devono avere un ciclo ricorsivo per attualizzare la valutazione fatta inizialmente a mano a mano che si procede con il progetto e vengono attuate le misure pianificate.
Le fasi del processo PIA possono essere condotte e registrate secondo il seguente schema:

1. VALUTAZIONE PRELIMINARE DI OPPORTUNITÀ PER UNA PIA. LA PRESENTE DPIA, TUTTAVIA, NON è STATA OGGETTO DI UNA VALUTAZIONE PRELIMINARE, IN CONSIDERAZIONE DELL'OBBLIGO POSTO DALLA LEGGE.

Questa fase serve a:

- spiegare ciò che il progetto intende realizzare,
- quali sono i benefici attesi per l'organizzazione,
- per gli individui e per le altre parti decidere, in base ad un insieme di domande mirate di screening, se un PIA sia necessario per dimensionare le risorse a seconda dell'entità del progetto e il tempo necessario alla valutazione capire gli impatti potenziali e i passi che potrebbero essere richiesti per identificare e ridurre il rischio.

2. DESCRIZIONE DEI FLUSSI DI INFORMAZIONI E COINVOLGIMENTO DEI PARTECIPANTI.

In questa fase si esegue una valutazione approfondita dei rischi e dei relativi impatti per la privacy e occorre valutare approfonditamente gli elementi che caratterizzano il trattamento dei dati descrivendo:

- quali informazioni sono utilizzate;
- come vengono trattate nelle singole fasi; cosa servono, ovvero per quale finalità; da chi sono ottenute, a chi sono comunicate; chi ne deve avere accesso.

In questa fase il processo di definizione della PIA può essere supportato da fonti informative già disponibili all'interno dell'organizzazione per descrivere come i dati saranno utilizzati, ad es. un diagramma che riporti i flussi informativi tra i vari soggetti o sistemi, la sequenza prevista delle operazioni di gestione dei dati, rapporti di audit sull'uso delle informazioni, mappe informative, registri di asset informativi.

Il DPO svolge un ruolo chiave con l'autorità di rivolgersi a chi è in grado di guidare le fasi della PIA sui processi esistenti ed inoltre può mantenere traccia di tutti le PIA eseguiti e di seguire le implicazioni derivanti dalla nuova procedura.

3. IDENTIFICAZIONE DEI RISCHI PRIVACY E DI QUELLI CORRELATI.

In questa fase occorre valutare gli aspetti di Privacy che espongono il progetto in esame a rischi di Privacy tenendo presente che il processo PIA è insieme una forma di risk assessment e di risk management per quanto riguarda le implicazioni specifiche di Privacy.
Dunque l'organizzazione deve considerare come il progetto specifico potrà generare eventuali problemi alla privacy degli interessati che, a loro volta, si ripercuoteranno sulla stessa organizzazione se non indirizzati correttamente, ad esempio un progetto che è intrusivo sul fronte del pubblico aumenta anche i rischi di multe, di danni reputazionali, o di perdite di operatività se rilasciato con carenze o soluzioni inappropriate.
Si deve procedere a identificare e gestire in modo sistematico l'insieme dei rischi, basandosi soprattutto su quanto svolto nella fase precedente di descrizione dei flussi informativi raggruppandoli in stadi di utilizzo dei dati come una sequenza logica dei trattamenti, da quando i dati vengono ricevuti dall'esterno a quando vengono aggregati, elaborati, storicizzati e poi ulteriormente trasferiti. È importante applicare a questi stadi un set di quesiti che consenta di far emergere le vulnerabilità e le minacce e su queste determinare gli effetti su cui quantificare gli impatti.
Laddove esistenti si possono utilizzare standard di settore o propri e metodologie di Project Management o di Risk Management per aiutarsi a categorizzare, identificare e misurare i rischi. Il rischio deve essere valutato in termini di coefficienti di probabilità e di gravità secondo scale numeriche associate a classi di valori.

4. INDIVIDUAZIONE DELLE SOLUZIONI E DELLE MISURE.

In questa fase le organizzazioni hanno bisogno di identificare quali soluzioni possono essere intraprese per i rischi che hanno identificato.
La PIA può offrire una serie di possibili opzioni per indirizzare ciascun rischio anche se va considerato che lo scopo non è quello di eliminare completamente l'impatto ma è quello di ridurre l'impatto ad un livello accettabile pur consentendo di realizzare un'iniziativa.
Dunque in questa fase, mentre si decide sulle possibili soluzioni, è sempre utile soppesare se gli scopi e i risultati del progetto sono proporzionati con l'impatto previsto sugli interessati e pertanto è opportuno tener traccia della misura di riduzione di rischio che ogni soluzione intende apportare.
Le organizzazioni hanno anche bisogno di valutare i costi e i benefici delle possibili soluzioni. Alcuni costi sono di natura prettamente finanziari, ad esempio quando deve essere acquistato un nuovo software per garantire un maggiore controllo sull'accesso e sulla conservazione, ma i maggiori costi devono essere bilanciati rispetto ai benefici attesi, come per esempio una maggiore garanzia per proteggersi da violazioni dei dati, un minore rischio di sanzioni o provvedimenti o di essere esposti ad effetti reputazionali.

5. APPROVAZIONE DELLE DECISIONI E REGISTRAZIONE DEI RISULTATI.

Per le soluzioni che si è deciso di portare avanti è opportuno tener traccia dei passi seguiti nel processo decisionale, compreso chi li abbia approvati.
Nei casi in cui si fosse deciso di accettare un rischio, dovrebbe essere esplicita l'argomentazione sostenuta e l'assunzione di responsabilità.

Si ritiene utile giungere alla conclusione delle attività producendo un report finale, da allegare alla documentazione di progetto, per riassumere il processo e i passi compiuti per mitigare il rischio privacy e per consentire di ricostruire a posteriori i motivi delle scelte fatte sulla base dei rischi individuati.
Si consideri che una registrazione del processo PIA può anche costituire una forma di comunicazione e di trasparenza verso gli interessati che ne richiedano la consultazione e diventare così una strategia di comunicazione, anche se il report PIA potrebbe non essere il solo documento prodotto come risultato del processo ma il PIA potrebbe aver fatto emergere il bisogno di una nuova comunicazione o regola da trasmettere agli interessati.

6. INTEGRAZIONE DEI RISULTATI DELLA PIA NEL PIANO DI PROGETTO.

I rilievi PIA e le azioni in esso previste dovrebbero essere integrati con il piano di progetto complessivo man mano che si sviluppa.
Anche se la maggior parte dell'impegno per la PIA risiede nelle fasi iniziali del progetto, potrebbe essere necessario ritornare alla PIA in vari stadi dello sviluppo e della realizzazione del progetto per avere conferma che le soluzioni sono state correttamente realizzate e hanno ottenuto l'effetto desiderato.
È probabile che i progetti di grande estensione ottengano benefici da un processo di revisione più formale.
Una PIA potrebbe generare azioni che continuano dopo che la valutazione è finita per cui è necessario che queste azioni vengano monitorate.

PARTE IV-VALUTAZIONE DEL CONTESTO

Mappatura dei rischi

1. PIANO D'AZIONE

Principi fondamentali: Nessun piano d'azione registrato.

Misure esistenti o pianificate: Nessun piano d'azione registrato.

Rischi: Nessun piano d'azione registrato.

2. DPO/RPD

Data Protection Officer è l'Avv. Luciano Paciello che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente indirizzo Email: lucianopaciello@avvocati1969.it PEC: lucianopaciello@pec.ordineavvocatitorino.it.

"Il DPO, sulla base dei documenti forniti dall'Ente e delle informazioni ottenute nel corso delle varie interlocuzioni avute con il Segretario Comunale, finalizzate alla ratifica della valutazione di impatto elaborata dal Comune di Terdobbiate, ritiene di poter convalidare la DPIA in oggetto.

Resta fermo il principio che detta valutazione, trattandosi di un'analisi dinamica e progressiva, dovrà essere aggiornata e/o integrata ad opera del Titolare del trattamento ogni qualvolta dovessero emergere nuove vulnerabilità nella sicurezza della gestione dei dati o qualora si dovesse verificare una evoluzione dello stato della tecnica, che renda disponibili, ad esempio, nuove possibilità di minimizzazione dei dati, ovvero nel caso in cui dovesse intervenire una modifica nei processi di trattamento di dati, tale da modificare i parametri utilizzati nella valutazione della DPIA in oggetto"

---

3. RICHIESTA DEL PARERE DEGLI INTERESSATI

Non è stato chiesto il parere degli interessati. L'atto organizzativo di adozione della procedura verrà trasmesso solo in informativa alle OO.SS. e R.S.U.

Motivazione della mancata richiesta del parere degli interessati: il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge.

Contesto-Panoramica del trattamento

1. QUALE È IL TRATTAMENTO IN CONSIDERAZIONE?

Sistema di Whistleblowing del Comune di Terdobbiate.

Esso svolge funzioni di segnalazione di illeciti per contrastare fenomeni corruttivi, sia nelle imprese private sia nelle pubbliche amministrazioni.

2. QUALI SONO LE RESPONSABILITÀ CONNESSE AL TRATTAMENTO?

- **Titolare del Trattamento** è il Comune di Terdobbiate (00545720039) nella persona del Sindaco pro tempore, Domenico Merisi. La sede legale è in Terdobbiate (NO) Via Roma, 28070, pec: terdobbiate@cert.ruparpiemonte.it, tel: 0321.84710.

- **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. Nominato dal Sindaco con accordo in data 24.08.2023 e trasmesso nella medesima data con prot. n. 3096.

- **Data Protection Officer** è l'Avv. Luciano Paciello che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente indirizzo Email: lucianopaciello@avvocati1969.it PEC: lucianopaciello@pec.ordineavvocatitorino.it.

- **Incaricato del trattamento**, per espressa previsione di legge, in quanto Responsabile della Prevenzione della Corruzione e Trasparenza è il Segretario del Comune di Terdobbiate, Dott.ssa Giuliana Balbo, in quanto persona fisica avente l'accesso esclusivo ai dati che pervengono attraverso i vari canali relativi a tutte le segnalazioni, comprese quelle in forma anonima.

3. CI SONO STANDARD APPLICABILI AL TRATTAMENTO?

Ai fini del rilevamento di illeciti penali si deroga dalla normativa in materia di protezione dei dati personali in quanto la materia di polizia giudiziaria è esclusa, come tutte le attività giurisdizionali, dal campo di applicazione del Reg. UE 2016/679 GDPR.
Per le altre attività si utilizzeranno le privacy polities indicate nel Registro del Trattamento, in particolare si applicheranno le linee guida del EDPB e del Garante nazionale per la protezione dei dati.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

Contesto-Dati, processi e risorse di supporto

1. QUALI SONO I DATI TRATTATI?

La piattaforma utilizzata, meglio definita in seguito, consente la compilazione, l'invio e la ricezione delle segnalazioni di presunti fatti illeciti nonché la possibilità per l'ufficio del Responsabile della prevenzione corruzione e della trasparenza (RPCT), che riceve tali segnalazioni, di comunicare in forma riservata con il segnalante senza conoscerne l'identità.

2. QUAL È IL CICLO DI VITA DEL TRATTAMENTO DEI DATI (DESCRIZIONE FUNZIONALE)?

Le segnalazioni non possono essere utilizzate oltre quanto necessario per dare adeguato seguito alle stesse. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, nonchè dagli articoli 5 e seguenti del decreto legislativo 14 marzo 2013, n. 33. Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo 24 del 2023 e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

3. QUALI SONO LE RISORSE DI SUPPORTO AI DATI?

I dati sono gestiti mediante l'uso della piattaforma informatica gratuita denominata "piattaforma WhistleblowingPA" per l'invio e la gestione in forma anonima delle segnalazioni così come previsto dal Decreto Legislativo 24 del 2023 e previsto dalle Linee Guida Anac.
La piattaforma è accessibile sul sito dell'ente al link: https://comunediterdobbiate.whistleblowing.it/ .
Il trattamento riguarda le segnalazioni ricevute dal RPCT attraverso la suddetta piattaforma.

WhistleblowingPA è un progetto di Transparency International Italia e Whistleblowing Solutions Impresa Sociale S.r.l. realizzato grazie al software GlobaLeaks, per l'acquisizione e la gestione - nel rispetto delle garanzie di riservatezza previste dalla normativa vigente - delle segnalazioni di illeciti da parte dei pubblici dipendenti e dai soggetti assimilati dalla normativa vigente.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

Principi Fondamentali-Proporzionalità e necessità

1.GLI SCOPI DEL TRATTAMENTO SONO SPECIFICI, ESPLICITI E LEGITTIMI?

Il trattamento in questione comporta il conferimento al Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell'ente, tramite compilazione di un form su apposita procedura web, di dati anagrafici, codice fiscale, dati di contatto e, eventualmente, dati sulla qualifica professionale, nonché di dati e informazioni ulteriori connessi alla condotta illecita riportata. I dati forniti verranno trattati esclusivamente per l'istruttoria della segnalazione ai sensi del Decreto Legislativo 24 del 10 marzo 2023.
Al fine di garantire la riservatezza del segnalante per tutta la durata della gestione della segnalazione, l'identità dello stesso sarà conosciuta solo dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell'ente. Ad eccezione dei casi in cui sia configurabile una responsabilità a titolo di calunnia e di diffamazione ai sensi delle disposizioni del codice penale o dell'art. 2043 del codice civile e delle ipotesi in cui l'anonimato non sia opponibile per legge (ad esempio, indagini penali, tributarie o amministrative, ispezioni di organi di controllo), l'identità del segnalante viene protetta in ogni contesto successivo alla segnalazione. Pertanto, fatte salve le citate eccezioni, l'identità del segnalante non può essere rivelata senza il suo espresso consenso, e tutti coloro che ricevono o sono coinvolti nella gestione della segnalazione sono tenuti a tutelare la riservatezza di tale informazione.
In questo ambito, i dati personali sono trattati dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) 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, ai sensi del D.Lgs n. 24 del 2023 avente ad oggetto: "Attuazione della direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, del 23.10.2019, 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" e delle Linee Guida whistleblowing approvate dall'ANAC con Delibera n. 311 del 12 luglio 2023.

Il trattamento dei dati personali è improntato ai principi di correttezza, liceità e trasparenza e di tutela della riservatezza e dei diritti dell'interessato, nonché agli ulteriori principi previsti dall'art. 5 del Regolamento.
Tali attività sono esplicitate attraverso specifica informativa ai sensi dell'articolo 13 del Regolamento Ue 679/2016

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

2.QUALI SONO LE BASI LEGALI CHE RENDONO LECITO IL TRATTAMENTO?

Il trattamento si basa sulle competenze attribuite dalla legge all'ente e, tra le altre, in particolare dal d.lgs.267/2000 "Testo Unico degli Enti Locali", dalla Legge 30 Novembre 2017, n. 179 “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.”, dalla Legge 6 Novembre 2012, n. 190 “Disposizioni per la prevenzione e la repressione della corruzione e della illegalità nella pubblica amministrazione.”, dal Decreto Legislativo 10 marzo 2023, n. 24 “Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.”

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

3. I DATI RACCOLTI SONO ADEGUATI, PERTINENTI E LIMITATI A QUANTO È NECESSARIO IN RELAZIONE ALLE FINALITÀ PER CUI SONO TRATTATI (MINIMIZZAZIONE DEI DATI)?

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all’articolo 5 , paragrafo 1, lettera c) RGPD, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l’utilizzazione dei dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l’interessato solo in caso di necessità.
Il trattamento dei dati personali verrà effettuato esclusivamente dal Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell’ente, con l’utilizzo di procedure anche informatizzate, dotate di strumenti di crittografia per garantire la riservatezza dell’identità del segnalante e del contenuto delle segnalazioni e della relativa documentazione, adottando misure tecniche e organizzative adeguate a proteggerli da accessi non autorizzati o illeciti, dalla distruzione, dalla perdita d’integrità e riservatezza, anche accidentali.

I dati verranno conservati per 5 anni e comunque per tutta la durata dell’eventuale procedimento disciplinare, penale o dinanzi la Corte dei Conti.
I dati personali non saranno comunicati ad altri soggetti, ad esclusione dei casi sopra indicati, così come non saranno oggetto di diffusione.

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

4. I DATI SONO ESATTI E AGGIORNATI?

Al fine della verifica della correttezza e dell'aggiornamento dei dati si stabilisce la prima verifica entro sei mesi dalla redazione del presente documento.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

5. QUAL È IL PERIODO DI CONSERVAZIONE DEI DATI?

Ai sensi dell'articolo 14 del D.Lgs. 24 del 10 marzo 2023 le segnalazioni, interne ed esterne, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, nel rispetto degli obblighi di riservatezza di cui all'articolo 12 del decreto legislativo citato e del principio di cui agli articoli 5, paragrafo 1, lettera e), del regolamento (UE) 2016/679 e 3, comma 1, lettera e), del decreto legislativo n. 51 del 2018.

Valutazione: *Accettabile.*

C**ommento di valutazione:** *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

PARTE V - MISURE A TUTELA DEGLI INTERESSATI

1. COME SONO INFORMATI DEL TRATTAMENTO GLI INTERESSATI?

Ai sensi dell'articolo 13 del D.Lgs. 24 del 10 marzo 2023, ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti viene 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.
I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.
I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del decreto legislativo 30 giugno 2003, n. 196, così come esplicitato fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché' adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.
I soggetti coinvolti 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, anche sulla base di questa specifica valutazione d'impatto sulla protezione dei dati, e disciplinando il rapporto con 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.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

2. OVE APPLICABILE: COME SI OTTIENE IL CONSENSO DEGLI INTERESSATI?

Il consenso degli interessati non è richiesto in quanto il fondamento giuridico del trattamento risiede nell'assolvimento di funzioni ed obblighi di legge.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

3.COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI ACCESSO E DI PORTABILITÀ DEI DATI?

In qualità di interessato si ha diritto di ottenere dall'ente, nei casi previsti dal Regolamento, l'accesso ai dati personali, la rettifica, l'integrazione, la cancellazione degli stessi o la limitazione del trattamento ovvero di opporsi al trattamento medesimo (artt. 15 e ss. del Regolamento). La richiesta potrà essere presentata, senza alcuna formalità, contattando direttamente il Responsabile della Prevenzione della Corruzione e della Trasparenza (RPCT) dell'ente all'indirizzo di posta elettronica personale disponibile alla home page dell'ente. Gli interessati che ritengano che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal Regolamento hanno, inoltre, il diritto di proporre reclamo all'Autorità Garante per la protezione dei dati personali, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento). Nella informativa presente sulla home page istituzionale dell'Ente è indicato il riferimento del titolare del trattamento, del DPO/RDP e del Garante Italiano per la protezione dei dati personali, con gli indirizzi mail e fisici, ai quali rivolgersi per avere informazioni ovvero per segnalare eventuali violazioni.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

4.COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI RETTIFICA E DI CANCELLAZIONE (DIRITTO ALL'OBLIO)?

Il diritto all'oblio si realizza automaticamente entro i termini previsti dalla norma per cui i dati sono conservati per cinque anni e comunque per tutta la durata dell'eventuale procedimento disciplinare.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

5.GLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO SONO DEFINITI CON CHIAREZZA E DISCIPLINATI DA UN CONTRATTO?

Sono contenute nell'atto di designazione a responsabile del trattamento e in quello di nomina a responsabile della prevenzione della corruzione e della trasparenza. Il contratto non è previsto in quanto egli è già legato da un rapporto contrattuale con l'Ente e pertanto la nomina e le indicazioni derivano da atto autoritativo di diritto amministrativo.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

6.IN CASO DI TRASFERIMENTO DI DATI AL DI FUORI DELL'UNIONE EUROPEA, I DATI GODONO DI UNA PROTEZIONE EQUIVALENTE?

Non è previsto alcun trasferimento al di fuori dell'Unione Europea.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

PARTE VI-VALUTAZIONE DEL SISTEMA

Rischi-Misure di sicurezza 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

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

2.SICUREZZA DEI DOCUMENTI CARTACEI

I documenti cartacei vengono conservati dal responsabile per la prevenzione della corruzione e della trasparenza e verifica che siano disposti in specifici raccoglitori in modo tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o i soggetti autorizzati.

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

3.SPECIFICHE MISURE DI SICUREZZA

Il Titolare del trattamento e il responsabile per la prevenzione della corruzione e della trasparenza, previa valutazione dei rischi, mettono in atto misure volte a:

- vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);
- impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);
- impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);
- impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente»);
- garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);
- garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);
- garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);
- impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);
- garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);
- garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

PER LE MISURE SPECIFICHE DI SICUREZZA RELATIVE ALL'UTILIZZO DELLA PIATTAFORMA INFORMATICA WHISTLEBLOWING PA SI RINVIA **AL DOCUMENTO ALLEGATO A.**

PER LE MISURE SPECIFICHE DI SICUREZZA RELATIVE AI DATI RACCOLTI IN DOCUMENTI CARTACEI SI SPECIFICA CHE:

1) I dati raccolti in verbale per le segnalazioni interne in forma orale sono conservati in armadio chiuso a chiave. La chiave dell'armadio in cui sono collocati i documenti è nella esclusiva disponibilità del RPCT.
2) I dati raccolti mediante compilazione di modulo per le segnalazioni in forma scritta, senza utilizzo della piattaforma, sono inseriti in busta chiusa e sigillata, indirizzata al Segretario Comunale, RPCT, all'indirizzo del Comune (Via Roma, 928070 Terdobbiate (NO) con indicazione in Stampatello "CONTENUTO RISERVATO – NON APRIRE - DA CONSEGNARE PERSONALMENTE AL RPCT". Nello specifico, le generalità del segnalante saranno inserite in una diversa busta, anch'essa chiusa e sigillata, inserita in quella più grande contenente la segnalazione. La busta verrà protocollata su disposizione del RPCT e conservata in armadio chiuso a chiave. La chiave dell'armadio in cui sono collocati i documenti è nella esclusiva disponibilità del RPCT. La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

Rischi-Accesso illegittimo ai dati

1. QUALI POTREBBERO ESSERE I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Qualora fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza, i dati sarebbero crittografati, Quindi si tratterebbe di un impatto limitato

2. QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONCRETIZZARE IL RISCHIO?

Furto o vandalismo.

3. QUALI SONO LE FONTI DI RISCHIO?

Interne ed esterne anche non umane.

4. QUALI MISURE FRA QUELLE INDIVIDUATE CONTRIBUISCONO A MITIGARE IL RISCHIO?

La piattaforma di segnalazione prevede

- **CRITTOGRAFIA**
  L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.
  Nessun dato viene salvato in chiaro su supporto fisico in nessuna delle fasi di caricamento

- **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.
  Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.
- **ARCHIVIAZIONE**
  L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM.
- **GESTIONE DELLE VULNERABILITÀ TECNICHE**
  L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review.
- **SICUREZZA DEI CANALI INFORMATICI**
  Tutte le connessioni sono protette
- **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.

I soggetti "autorizzati" a trattare i dati sono nominati con specifici atti sono istruiti e formati sul corretto trattamento.

Per i dati contenuti in documenti cartacei: controllo degli accessi fisici, tracciabilità, minimizzazione dei dati, sicurezza dei documenti cartacei mediante chiusura dei dati in busta sigillata e in armadio chiuso a chiave, prevenzione delle fonti di rischio.

COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Limitato, poiché il sistema di crittografia, l'utilizzo del PC personale del RPCT protetto da password di accesso (conosciuta solo dal RPCT), il controllo degli accessi fisici ai documenti cartacei, con le modalità descritte nella sezione specifiche misure di sicurezza, rendono molto limitato il rischio di accesso abusivo ai dati e limitato il rischio di distruzione degli stessi.

5. COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Limitata, sulla base delle misure pianificate.

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Rischi-Modifiche indesiderate dei dati

1. QUALI SAREBBERO I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

L’impatto va valutato anche alla stregua di quanto previsto dall’articolo 12 del D.Lgs 24 del 10/03/2023 dove si sottolinea che l’identità della persona segnalante non può essere rivelata, senza il consenso espresso della stessa persona segnalante, a persone diverse da quelle competenti a ricevere o a dare seguito alle segnalazioni, espressamente autorizzate a trattare tali dati ai sensi degli articoli 29 e 32, paragrafo 4, del regolamento (UE) 2016/679 e dell'articolo 2-quaterdecies del codice in materia di protezione dei dati personali di cui al decreto legislativo 30 giugno 2003, n. 196.
Allo stesso modo va valutato il tipo di procedimento che scaturisce dalla segnalazione.
Nell'ambito del procedimento penale, l’identità della persona 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 della persona segnalante non può essere rivelata fino alla chiusura della fase istruttoria.
Nell'ambito del procedimento disciplinare, l’identità della persona 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 della persona segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza del consenso espresso della persona segnalante alla rivelazione della propria identità

2. QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA CONCRETIZZAZIONE DEL RISCHIO?

Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

3. QUALI SONO LE FONTI DI RISCHIO?

Fonti umane interne, fonti umane esterne, fonti non umane.

4. QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Controllo degli accessi logici, controllo degli accessi fisici, tracciabilità, minimizzazione dei dati, sicurezza dei documenti cartacei, prevenzione delle fonti di rischio.

5. COME STIMERESTE LA GRAVITÀ DEL RISCHIO, IN PARTICOLARE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Limitata, il sistema di crittografia e il controllo logico degli accessi rende pressoché impossibile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti.

6. COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO A MINACCE, FONTI DI RISCHIO E MISURE PIANIFICATE?

Limitata, in considerazione del controllo degli accessi logici, della crittografia dei dati e dei sistemi di sicurezza fisica e di allarme.

Valutazione: *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Rischi-Perdita di dati

1. QUALI POTREBBERO ESSERE GLI IMPATTI PRINCIPALI SUGLI INTERESSATI SE IL RISCHIO DOVESSE CONCRETIZZARSI?

Impossibilità di recuperare le segnalazioni e i dati dei soggetti segnalanti.

2. QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA MATERIALIZZAZIONE DEL RISCHIO?

Errore materiale, furto o vandalismo, danno o malfunzionamento del sistema di registrazione dei dati.

3. QUALI SONO LE FONTI DI RISCHIO?

Fonti umane interne, fonti umane esterne, fonti non umane.

4. QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Controllo degli accessi logici, controllo degli accessi fisici, tracciabilità, minimizzazione dei dati, sicurezza dei documenti cartacei, prevenzione delle fonti di rischio.

5. COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Per le segnalazioni mediante piattaforma informatica molto limitata, in quanto i sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

Per segnalazioni su supporto cartaceo limitata perché i dati sono raccolti in buste sigillate e sono conservate in armadio chiuso a chiave. La chiave dell'armadio in cui sono collocati i documenti è nella esclusiva disponibilità del RPCT. La segnalazione è poi oggetto di protocollazione riservata, anche mediante autonomo registro, da parte del gestore.

6. COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Limitata, i sistemi di sicurezza adottati rendono trascurabile il rischio.

Valutazione: *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

PARTE VII-INDICAZIONI DI SICUREZZA

Vigilanza, adeguamento e verifica

1. FORMAZIONE

L'obbligo di formazione previsto dalla vigente normativa (art.29 e 32 Reg.UE 2016/679 GDPR) che costituisce un dovere generale nell'ambito del principio di accountability, rende necessario un percorso di aggiornamento per estendere a tutti i soggetti coinvolti, in ogni modo, la conoscenza e le cautele da adottare per la corretta gestione del trattamento dei dati.

2. VERIFICA

La nuova normativa, a partire dal 14 luglio 2023, richiede la verifica dell'efficienza ed efficacia delle valutazioni eseguite in questa valutazione d'impatto e il riscontro all'atto del funzionamento operativo.

Allo scopo si suggerisce di prevedere:

− una verifica ispettiva a 6 mesi dall'attivazione del sistema; −
Un ciclo di visite ispettive di verifica almeno annuali.

Terdobbiate (NO),

Il Titolare del trattamento

Domenico Merisi

Signed by: MERISI DOMENICO
Issuer: InfoCamere Qualified Electronic Signature CA
Signing time: 01-12-2023 09:48 UTC +01

Il Responsabile del trattamento
Responsabile per la prevenzione della corruzione e della trasparenza

Dott.ssa Giuliana Balbo

Firmato digitalmente da
Giuliana Balbo
CN = Balbo Giuliana
C = IT

Il RDP/DPO

Avv. Luciano Paciello

PACIELLO
LUCIANO
Avvocato
28.11.2023
14:39:41
GMT+01:00