Comune di Limena

Provincia di Padova

Limena -via Roma, 44 cap. 35010 c.f. e p.iva 00327150280 - http://www.comune.limena.pd.it – fax 049/8841277 - 049/8840426
telefoni: segreteria 049.8844338 – lavori pubblici 049.8844344 – edilizia privata 049.8844348 – assistente sociale 049.8844313

Limena, 20/12/2023
Prot. come da segnatura prot. n. 0018740 del 20-12-2023 interno

GESTIONE DELLE SEGNALAZIONI WHISTLEBLOWING

Documento di valutazione di impatto sui diritti e le libertà degli interessati oggetto di trattamento

Introduzione

Il Titolare del trattamento, considerato l'obbligo normativo di cui agli artt. 35 Regolamento (UE) 2016/679 (recante disposizioni relative alla valutazione di impatto sulla protezione del dato personale) e 13, co. 6 d.lgs. 24/2023, ha ritenuto necessario procedere ad una valutazione d'impatto sul trattamento denominato "Gestione delle segnalazioni *whistleblowing*".

Definizioni

Titolare del trattamento: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri.

Interessato (del trattamento): soggetto al quale si riferiscono i dati personali, persona fisica identificata o identificabile. Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Dato personale: qualsiasi informazione riguardante un interessato.

Valutazione di impatto sul dato personale: procedura prevista dall'articolo 35 del Regolamento UE/2016/679 che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli. La DPIA può riguardare un singolo trattamento oppure più trattamenti che presentano analogie in termini di natura, ambito, contesto, finalità e rischi.

Danno: effetto negativo determinato dal verificarsi di una minaccia. Il danno è causato dalla compromissione del dato personale dell'interessato nelle tre dimensioni di riservatezza, disponibilità ed integrità.

Minaccia: evento potenzialmente dannoso che, se verificato, pone in pericolo i dati personali dell'interessato, con ricadute sui suoi diritti e le sue libertà, causando un danno.

Rischio potenziale: ponderazione del danno per la probabilità statistica che l'evento avverso accada. Si tratta di un indice creato per poter confrontare eventi (in questo contesto le minacce) che hanno diverse probabilità di accadimento e diverse dimensioni del danno.

Contromisura: misura in grado di mitigare il rischio, riducendo la probabilità di accadimento della minaccia.

Vulnerabilità: rappresentano delle situazioni che innalzano la probabilità del rischio sul dato personale.

Rischio reale: è il rischio potenziale, mitigato dallo stato di protezione del dato personale, cioè, diminuito dalle contromisure già adottate e aumentato dalle vulnerabilità presenti.

Piano del trattamento del rischio: piano di progettazione operativo con il quale si individuano le contromisure da implementare, nonché il grado di maturità di quelle già attuate, necessarie per abbassare il rischio reale al di sotto della soglia "alto"

Rischio residuo: è il rischio reale, mitigato dallo stato futuro di protezione del dato personale. Esso si potrà ottenere a seguito dell'attuazione del piano del trattamento del rischio.

PANORAMICA DEL TRATTAMENTO (*art. 35, par. 7, lett. a) Reg. UE 2016/679*)

Il presente verbale descrive la valutazione di impatto sulla protezione del dato personale effettuata sui trattamenti come di seguito indicati.

Nella fattispecie concreta, sulla base della tipologia di trattamento eseguito, il grado di compromissione dei dati sarà considerato come la probabilità di accadimento di un una o più minacce e l'impatto derivante dal verificarsi di una minaccia in relazione ai diritti e le libertà dell'interessato. Maggiore è il grado di compromissione, maggiore sarà la probabilità di rischio per i diritti e le libertà dell'interessato.

Nella fattispecie si considerano rischi:

• Rischio che a causa del trattamento derivi un danno reputazionale all'interessato. Si pensi, in questo frangente, ad una violazione che comporti la perdita di riservatezza delle informazioni riferite alla persona fisica coinvolta.

• Rischio di discriminazione (a scuola, a lavoro, ecc.) derivante dal trattamento. Come nel precedente punto, il rischio di discriminazione può derivare dalla perdita di riservatezza del dato personale, ma anche nella menomazione della sua integrità, laddove un'informazione sia stata acquisita o registrata in modo non accurato.

• Rischio di subire un furto di identità a causa del trattamento. Tale rischio si lega specificamente alla perdita di riservatezza e di disponibilità del dato personale, ed è legato essenzialmente alla natura di bene personalissimo connessa al dato personale (che per sua natura è indisponibile).

• Rischio che il trattamento comporti delle perdite finanziarie all'interessato, valutando anche l'eventuale danno da perdita di chance laddove, ad esempio, il trattamento comporti l'esclusione dalla possibilità di gestire alcuni affari. Il rischio è sicuramente connesso alla perdita di riservatezza ed integrità dei dati personali coinvolti nel trattamento.

• Rischio di subire danni fisici o psicologici come conseguenza del trattamento; si pensi ad un ospedale che perda i dati della cartella clinica di un paziente di lì a poco soggetto ad intervento.

• Rischio di perdita del controllo dei dati, laddove l'interessato, a causa del trattamento, non possa più disporre liberamente di alcune sue informazioni personali (si pensi, ad esempio, al problema dell'acquisizione e diffusione di immagini personali da parte di un paparazzo).

• Rischio di subire svantaggi economici e sociali.

• Rischio di trovarsi nell'impossibilità di esercitare alcuni diritti. Si deve ricordare, infatti, come la tutela dei dati personali sia costituzionalmente riconosciuta come diritto prodromico al corretto esercizio di tutte le altre libertà e diritti riconosciuti dall'ordinamento (nazionale ed europeo).

Il Titolare del trattamento è chiamato ad esprimersi sulle conseguenze (impatto) che si potrebbero verificare in termini di danno (fisico, materiale, immateriale) qualora i dati personali venissero persi, distrutti e quindi non più disponibili, modificati e diffusi, ossia portati a conoscenza o comunicati a soggetti non autorizzati. In particolare, il Titolare del trattamento è chiamato ad individuare anche la probabilità che detto rischio ha di verificarsi.

Per effettuare la valutazione d'impatto con cognizione di causa, l'Ente ritiene opportuno esplicitare le minacce che potrebbero avverarsi nell'ambito dello specifico trattamento sottoposto a DPIA.

Le minacce prese in considerazione sono elencate di seguito.

Elenco minacce:

- Uso non autorizzato della strumentazione;
- Alterazione volontaria e non autorizzata di dati di business;
- Virus (malware);
- Accesso non autorizzato alla rete;
- Uso non autorizzato della rete da parte degli utenti;
- Trattamento (volontario o inconsapevole) non consentito di dati (personali);
- Errori degli utenti;
- Uso dei servizi da parte di persone non autorizzate;
- Degrado dei supporti di memorizzazione/conservazione;
- Uso dei servizi in modo non autorizzato;
- Furto d'identità;
- Intercettazione, inclusa l'analisi del traffico;
- Furto di documenti o supporti di memorizzazione;
- Recupero di informazioni da media (principalmente memorie di massa) dismessi;
- Rivelazione di informazioni (da parte del personale o dei fornitori);
- Infiltrazione nelle comunicazioni;
- Incendio;
- Allagamento;
- Polvere, corrosione, congelamento;
- Attacchi (bombe, terroristi);
- Fulmini e scariche atmosferiche;
- Fenomeni climatici (uragani, nevicate);
- Terremoti, eruzioni vulcaniche;
- Guasto aria condizionata o sistemi di raffreddamento;
- Malfunzionamento nei componenti di rete;
- Errori di trasmissione (incluso il *misrouting*);
- Interruzione nei collegamenti di rete;
- Interruzione di servizi erogati riconducibili ai fornitori esterni (inclusi ISP, CSP, DR site, supporto tecnico specialistico, esternalizzazione attività). Per esempio, a causa di fallimento, chiusura, cessazione del fornitore;
- Indisponibilità del personale (malattie, sciopero, ecc.);

- Perdita di fornitori, fallimento, incidenti;
- Errori dei componenti TLC;
- Eccesso di traffico sulle linee TLC;
- Fault o malfunzionamento della strumentazione IT;
- Errori di manutenzione hardware e software di base;

Elenco delle contromisure adottate dall'Ente:

- Formazione di base del personale deputato alla gestione delle segnalazioni (sia in ambito privacy, sia in ambito anticorruzione);
- Utilizzo di credenziali sicure (lunghezza di almeno 12 caratteri) per l'accesso alla piattaforma informatica;
- Crittografia (piattaforma informatica);
- Controllo degli accessi logici (piattaforma informatica);
- Prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza (piattaforma informatica);
- I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery (piattaforma informatica);
- Procedura per la gestione del *data breach* (Responsabile del trattamento);
- Inferriate alle finestre (con riferimento all'ufficio del RPCT);
- Porte con serratura (con riferimento all'ufficio del RPCT);
- Impianto d'allarme (con riferimento al locale ove verrà conservata la segnalazione cartacea, se previsto);
- Parafulmine;

PANORAMICA DEL TRATTAMENTO

Il trattamento sottoposto a valutazione d'impatto (c.d. D.P.I.A.) riguarda la gestione delle segnalazioni in materia di *whistleblowing*; nello specifico, verrà presa in considerazione la gestione del c.d. canale di segnalazione interno, il quale consente di inoltrare le segnalazioni provenienti dal *whistleblower* (dipendenti pubblici, intesi in senso ampio e collaboratori della pubblica amministrazione), al responsabile della prevenzione e della corruzione (RPCT).

I canali di segnalazione interna messi a disposizione dall'Ente sono i seguenti:

- piattaforma informatica;

- incontro diretto con il RPCT, fissato entro un termine ragionevole (come indicato nell'atto organizzativo, la segnalazione verrà effettuata oralmente in presenza del RPCT e, successivamente, verrà redatto apposito verbale con sottoscrizione sia del segnalante sia del RPCT; il verbale verrà conservato in luogo idoneo a garantirne la segretezza).

Natura dei dati

Considerato che la normativa di riferimento (d.lgs. 24/2023) stabilisce che la segnalazione consiste nella "comunicazione scritta od orale di informazioni sulle violazioni" e che per informazioni sulle violazioni si intendono tutte le "informazioni, compresi i fondati sospetti, riguardanti violazioni commesse o che, sulla base di elementi concreti, potrebbero essere commesse nell'organizzazione con cui la persona segnalante o colui che sporge denuncia all'autorità giudiziaria o contabile intrattiene un rapporto giuridico ai sensi dell'articolo 3, comma 1 o 2, nonché gli elementi riguardanti condotte volte ad occultare tali violazioni", la ricezione e la gestione delle segnalazioni dà luogo al trattamento di dati personali c.d. "comuni"; può dar luogo, a seconda del contenuto delle segnalazioni e degli atti e documenti allegati, a trattamenti di dati

personali c.d. particolari (*ex* art. 9 Reg. UE 2016/679) e di dati personali relativi a condanne penali e reati (*ex* art. 10 Reg. UE 2016/679).

Ciclo di vita del trattamento

L'art. 14 del d.lgs. 24/2023, rubricato "conservazione della documentazione inerente alle segnalazioni", stabilisce che 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 [...]". In conseguenza di ciò, il ciclo di vita dei dati personali trattati in occasione di una segnalazione di *whistleblowing* ha inizio dalla data di ricevimento della segnalazione (è direttamente il *whistleblower* ad effettuare la comunicazione di dati personali, propri e delle persone coinvolte nella segnalazione) e terminerà decorsi 5 anni dalla data della comunicazione dell'esito finale della procedura di segnalazione (termine massimo entro il quale il Titolare può conservare la segnalazione e la documentazione ad essa allegata); si veda l'art. 14, co. 1 d.lgs. 24/2023.

Risorse di supporto dei dati

Con riferimento alle segnalazioni effettuate mediante piattaforma informatica, *Whistleblowing Solutions Impresa Sociale S.r.l.* si avvale di Seeweb S.R.L., qualificata come *sub*-responsabile del trattamento, per procedere all'archiviazione in cloud dei dati. I dati sono salvati con backup giornaliero incrementale su Data Center delocalizzato basato su Veeam Backup & Replication con 7 *restore point*. Tutti i datacenter dai quali sono erogati i servizi sono situati sul territorio italiano e posti ad elevata distanza, tale da assicurare la completa indipendenza dei domini di disastro secondo le normative internazionali. Tutti i datacenter sono di proprietà e in completa gestione del fornitore.

Finalità del trattamento

Le finalità del trattamento consistono nella gestione delle segnalazioni di whistleblowing, a prescindere dalla modalità con la quale sono pervenute all'Ente. Qualsiasi segnalazione, a meno che non si tratti di notizie palesemente prive di fondamento, di informazioni che sono già totalmente di dominio pubblico o di informazioni acquisite solo sulla base di indiscrezioni o vociferazioni scarsamente attendibili (c.d. voci di corridoio), deve essere istruita dal RPCT al fine di accertare la veridicità di quanto segnalato. Nel caso dovesse risultare necessario, il RPCT potrà comunicare l'esito dell'accertamento all'ANAC, all'autorità giudiziaria o attivare il procedimento disciplinare nei confronti del segnalato o del segnalante.

Basi giuridiche del trattamento

I dati forniti vengono trattati per svolgere l'istruttoria della segnalazione e dar seguito alla stessa, ai sensi dell'art. 5 del d.lgs. 24/2023, allo scopo di accertare eventuali violazioni delle norme previste dal decreto *whistleblowing*. La base giuridica di tale trattamento è quindi rappresentata dall'art. 6, par. 1, lett. c) del Regolamento UE 2016/679 ("il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento").

Nei casi di cui all'art. 12, commi 3, 4 e 5 d.lgs. 24/2023, può presentarsi la necessità di rivelare l'identità della persona segnalante; nel caso previsto dal comma 5, per poter palesare l'identità del segnalante è necessario chiedere il consenso a quest'ultimo. In questo caso, pertanto, la base giuridica del trattamento è rappresentata dall'art. 6, par. 1, lett. a) del Regolamento UE 2016/679 ("l'interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità"). L'Ente, nell'informativa messa a disposizione dell'interessato da evidenza che il mancato consenso a tale rivelazione comporterà, in ambito disciplinare, l'inutilizzabilità della segnalazione, ponendo fine al procedimento in corso; in secondo luogo,

l'Ente ricorda che, ai sensi dell'art. 7, par. 3, Regolamento UE 2016/679, "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca."

I dati sono adeguati, pertinenti e limitati

I dati sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per cui sono trattati. La normativa di riferimento e le linee guida ANAC chiariscono che le violazioni segnalate devono essere circostanziate il più possibile per consentire un'agevole verifica e analisi dei fatti descritti nella segnalazione.

I dati sono esatti ed aggiornati

I dati sono esatti e, se necessario, aggiornati come previsto dall'art. 5 par. 1 lett. e) del Regolamento UE 2016/679. Anche nel caso in cui la segnalazione dovesse pervenire per mezzo della piattaforma elettronica adottata dall'Ente, il *whistleblower*, grazie al *key code* generato all'esito della procedura di segnalazione, ha sempre la possibilità di aggiornare i dati ed il contenuto della segnalazione.

Periodo di conservazione dei dati

Come previsto dall'art. 13 del d.lgs. n. 24 del 10 marzo 2023, 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 di comunicazione dell'esito finale della procedura di segnalazione nel rispetto degli obblighi di cui all'art. 12 del d.lgs. 10 marzo 2023 n. 24 e del principio di cui agli articoli 5 par. 1 lett. e) del Reg. UE 2016/679.

Informativa e consenso

Viene resa apposita informativa ex art. 13 Reg. UE 2016/679. Questa è pubblicata sul sito istituzionale dell'Ente e, inoltre, viene consegnata in versione cartacea nell'ipotesi in cui il *whistleblower* richieda l'incontro diretto con il RPCT.

Considerata l'ipotesi disciplinata dall'art. 12, co. 5 d.lgs. 24/2023, nell'informativa messa a disposizione dell'interessato l'Ente da evidenza che il mancato consenso alla rivelazione dell'identità del segnalante comporterà, in ambito disciplinare, l'inutilizzabilità della segnalazione, ponendo fine al procedimento in corso; in secondo luogo, l'Ente ricorda che, ai sensi dell'art. 7, par. 3, Regolamento UE 2016/679, "L'interessato ha il diritto di revocare il proprio consenso in qualsiasi momento. La revoca del consenso non pregiudica la liceità del trattamento basata sul consenso prima della revoca."

Responsabili del trattamento

Viene individuato quale Responsabile del trattamento la Società *Whistleblowing Solutions S.I. S.R.L.* che fornisce la piattaforma informatica per la gestione delle segnalazioni; come sub-responsabili del trattamento viene individuata Seeweb S.R.L., nominata da *Whistleblowing Solutions S.I. S.R.L. e Transparency International Italia*, nominato "per la collaborazione nella gestione del sistema di *whistleblowing*".

Destinatari di paesi terzi

I dati non vengono trasferiti in Paesi terzi.

VALUTAZIONE D'IMPATTO

DISPONIBILITÀ DANNI FISICI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): **BASSO**

- Probabilità di avverarsi dell'evento (rischio): **IMPROBABILE**

DISPONIBILITÀ DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (impatto): **BASSO**

- Probabilità di avverarsi dell'evento (rischio): **IMPROBABILE**

DISPONIBILITÀ DANNI IMMATERIALI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero PERSI O DISTRUTTI IRRIMEDIABILMENTE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): **MEDIO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

INTEGRITÀ DANNI FISICI

Quale potrebbe essere il danno all'interessato se di dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): **BASSO**

- Probabilità di avverarsi dell'evento (rischio): **IMPROBABILE**

INTEGRITÀ DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se di dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di

avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (Impatto): **BASSO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

INTEGRITÀ DANNI IMMATERIALI

Quale potrebbe essere il danno all'interessato se di dati dello stesso venissero MODIFICATI IN MANIERA INDESIDERATA durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): **MEDIO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

RISERVATEZZA DANNI FISICI

Quale potrebbe essere il danno all'interessato se i dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un DANNO FISICO? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI FISICI all'interessato (impatto): **BASSO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

RISERVATEZZA DANNI MATERIALI

Quale potrebbe essere il danno all'interessato se di dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire perdite finanziarie, o altri svantaggi economici o sociali? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI MATERIALI all'interessato (Impatto): **MEDIO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

RISERVATEZZA DANNI IMMATERIALI

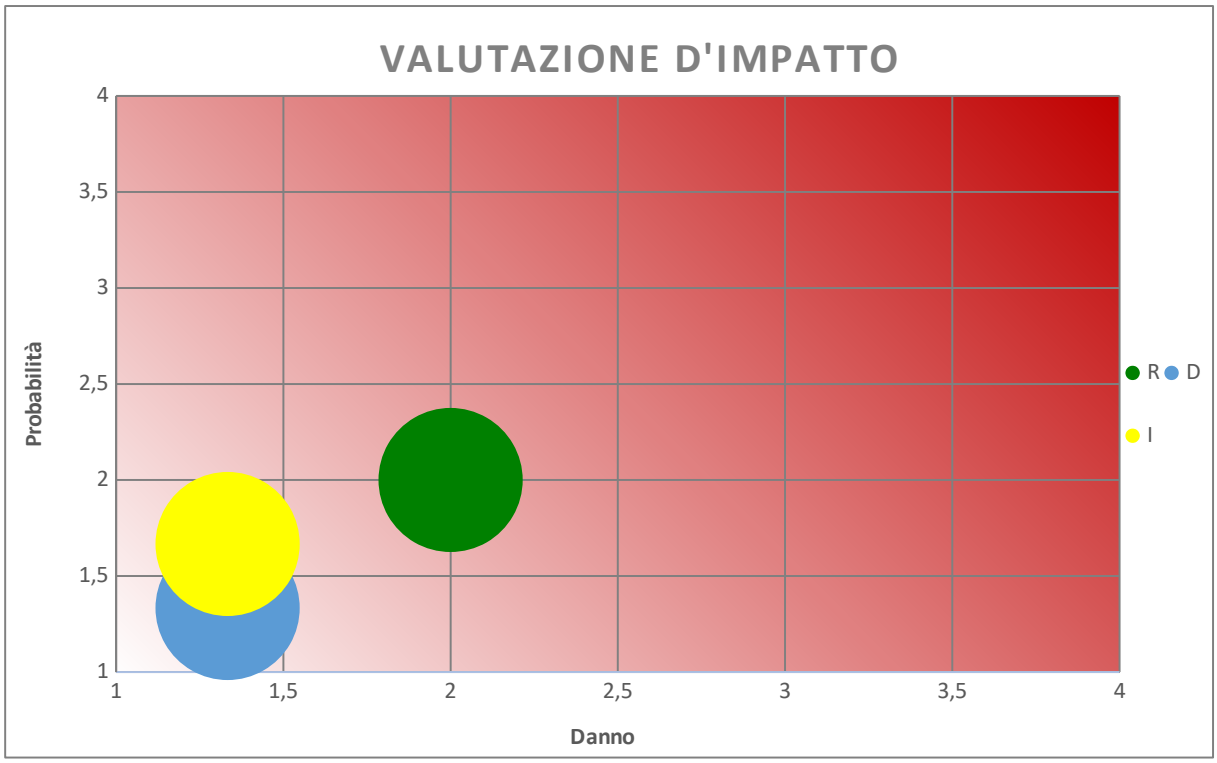
Quale potrebbe essere il danno all'interessato se di dati dello stesso venissero DIFFUSI O COMUNICATI A PERSONE NON AUTORIZZATE durante l'esecuzione delle finalità di trattamento interessate alla valutazione? L'interessato potrebbe subire un danno reputazionale, perdita del controllo dei dati, impossibilità di esercitare i diritti, discriminazione, furto di identità? Come definirebbe la probabilità di avverarsi dell'evento anche in considerazione al grado di compromissione dei dati della vostra organizzazione?

- Livello di rischio di DANNI IMMATERIALI all'interessato (impatto): **ALTO**

- Probabilità di avverarsi dell'evento (rischio): **POCO PROBABILE**

MAPPATURA DEL RISCHIO

Nel grafico sottostante è riportato il valore reale dell'impatto sui diritti e le libertà dell'interessato a cui appartengono i dati personali trattati dall'Ente durante le attività di trattamento sottoposte ad analisi.



Legenda:

R = riservatezza

D = disponibilità

I = integrità

} caratteristiche del dato personale

Documenti allegati:

- Atto organizzativo per la gestione del canale interno;
- Documentazione tecnica a supporto del Titolare nella valutazione d'impatto sulla protezione dei dati, fornita dal Responsabile del trattamento sopra indicato.

IL TITOLARE DEL TRATTAMENTO
Il Sindaco
Stefano Tonazzo
(documento firmato digitalmente)

WHISTLEBLOWINGIT

DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

TRATTAMENTO DATI RELATIVI ALLE SEGNALAZIONI DI CONDOTTE ILLECITE (C.D. WHISTLEBLOWING)

Documento aggiornato il 15 luglio 2023

WHISTLEBLOWINGIT
Un progetto di Whistleblowing Solutions Impresa Sociale e Transparency International Italia
www.whistleblowing.it | info@whistleblowing.it

SOMMARIO

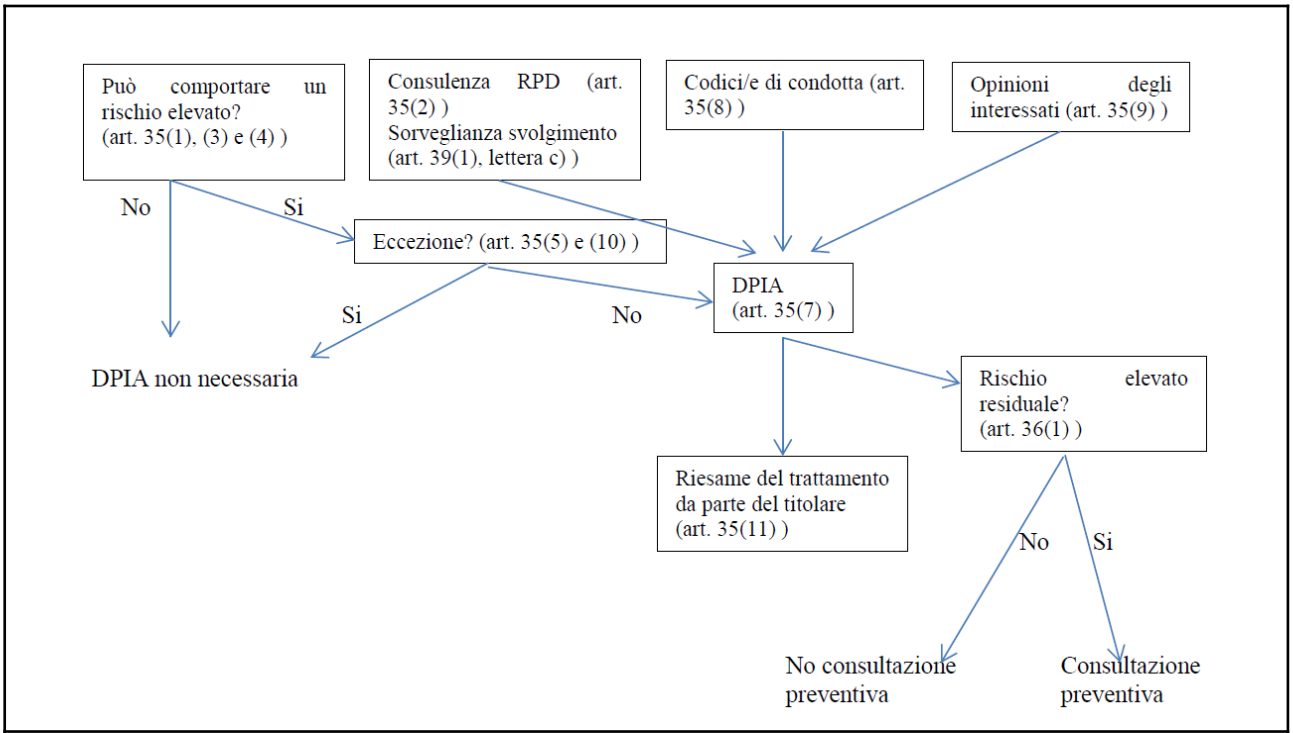
1. PREMESSA

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.

Whistleblowing Solutions, nel suo ruolo di Responsabile del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.



Principi fondanti il processo di DPIA

2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

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.

ARCHITETTURA DI SISTEMA

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.

SOFTWARE IMPIEGATO

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

In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile. Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

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

- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

Predisposizione dei sistemi virtualizzati:

- I server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
- Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);

- Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
- Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

ARCHITETTURA DI RETE

- L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- Ogni connessione di rete implementa TLS 1.2+;
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità;
- 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.

3. DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento:	**PA, Ente o Organizzazione** > Titolare del trattamento **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing **Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) **Transaparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing **Conformità normativa:**
Standard applicabili:	• ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks" • ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud • ISO27018 per la protezione dei dati personali nei servizi Public Cloud • Qualifica AGID • Certificazione CSA Star
Dati e operazioni di trattamento:	Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti. **Dati di registrazione** Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). **Categorie particolari di dati** Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. **Dati relativi a condanne penali e reati** Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento e dei dati	1) Attivazione della piattaforma 2) Configurazione della piattaforma 3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti 4) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore
Risorse a supporto delle attività di trattamento:	Software di whistleblowing professionale GlobaLeaks Infrastruttura IaaS e SaaS privata basata su tecnologie: - Dettaglio Hardware - VMWARE (virtualizzazione) - Debian Linux LTS (sistema operativo) - VEEAM (backup) - OPNSENSE (firewall) - OPENVPN (vpn)

4. VALUTAZIONI IN MERITO AI TRATTAMENTI

PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Esattezza e aggiornamento dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte.

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

Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti	Gli accordi contrattuali sono definiti con le seguenti società: • Whistleblowing Solutions in qualità di Responsabile del trattamento • Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions • Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions

Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:	I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

5. MISURE DI SICUREZZA

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

CONTROLLO DEGLI ACCESSI LOGICI

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

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.

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.

GESTIONE DELLE VULNERABILITÀ TECNICHE

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

A questi si aggiunge la peer review indipendente realizzata dalla 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

BACKUP

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

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.

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.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7×24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7×24.

I datacenter del fornitore IaaS sono certificati ISO27001.

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.

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.

6. MISURE ADDIZIONALI

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

- THREAT MODEL
- APPLICATION SECURITY