Comune di Candiolo

Città Metropolitana di Torino

Valutazione d'impatto (DPIA) circa i canali di segnalazione interna Whistleblowing

Redattore
Titolare del Trattamento - Comune di Candiolo
Revisore
Studio Pacchiana Parravicini e Associati
Validatore
DPO – Avv. MICHELA Cristiano

Il sottoscritto Avv. MICHELA Cristiano in qualità di DPO dell'Ente valida il seguente documento di Valutazioned'impatto con riferimento ai canali di segnalazione interna whistleblowing implementati dal Comune di Candiolo.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

La presente DPIA ha ad oggetto il trattamento dei dati personali raccolti mediante l'uso dei canali di segnalazione interna che il Comune di Candiolo ha deciso di implementare per rispettare quanto previsto dal D.lgs. 24/2023 che disciplina la protezione delle persone che segnalano violazioni del diritto dell'Unione e la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

In particolare, il Comune di Candiolo ha previsto il seguente Canale di segnalazione interna:

- in forma scritta con canale informatico-elettronico mediante uso della piattaforma WhistleblowingPA.

Tutta l'attività svolta dal RPCT è conforme alleLinee Guida A.N.AC. adottate con delibera n. 311 del 12 luglio 2023.

Quali sono le responsabilità connesse al trattamento?

Il **Titolare del trattamento è** il Comune di Candiolo, sedente in Candiolo (TO), Via Ugo Foscolo, 4.

Con riferimento al Canale di segnalazione in forma scritta il **Responsabile del trattamento** (per la fornitura e la gestione della piattaforma WhistleblowingPA) è la **WhistleblowingSolutions.**

Whistleblowing Solutions ha nominato – sulla base dell'autorizzazione fornita dal Titolare (cfr. Art. 5 della Nomina ex art. 28 del GDPR) - due **sub-responsabili**:

- **Seeweb** per la gestione dell'infrastruttura della piattaforma WhistleblowingPA (IaaS);

- **Transaparency International Italia** per la collaborazione nella gestione del sistema della piattaforma WhistleblowingPA.

Ci sono standard applicabili al trattamento?

Sono applicabili al trattamento i seguenti standard nazionali:

- **ISO27001** per l'"Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks";
- **ISO27017** per i 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.**

Valutazione della sezione: Accettabile

Contesto

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Nella gestione delle segnalazioni, presentate per il tramite del canale già indicato, verranno trattate le seguenti categorie di dati personali:

• Dati personali comuni

In particolare, si tratta dei dati identificativi del segnalante oppure dei dati di contatto dei referenti del Titolare che attiva il servizio di digital whistleblowing (es. Responsabile Anticorruzione).

• Dati particolari

In particolare, si tratta dei dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati.

• **Dati relativi a condanne penali e reati**

In particolare, si tratta dei dati eventualmente contenuti nella segnalazione e in atti edocumenti ad essa allegati.

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

Sia in caso di segnalazione scritta sia in caso di segnalazione orale, i dati vengo trattati secondo le seguenti attività:

- **Raccolta:** attività di acquisizione del dato;
- **Registrazione:** memorizzazione dei dati su un qualsiasi supporto;
- **Organizzazione:** classificazione dei dati secondo un metodo prescelto;
- **Conservazione:** attività consistente nel mantenere memorizzate le informazioni su un qualsiasi supporto;
- **Consultazione:** lettura dei dati personali;
- **Selezione:** individuazione di dati personali nell'ambito di gruppi di dati già memorizzati;
- **Estrazione:** attività di estrapolazione di dati da gruppi già memorizzati;
- **Raffronto:** è un'operazione di confronto tra dati, sia una conseguenza di elaborazione che di selezione o consultazione.
- **Utilizzo:** attività generica che ricopre qualsiasi tipo di impiego dei dati;
- **Cancellazione:** eliminazione di dati tramite utilizzo di strumenti elettronici;
- **Distruzione**: eliminazione definitiva dei dati.

Con riferimento al trattamento dei dati ottenuti mediante canale interno in forma scritta, si segnala chela piattaforma Web Whistleblowing PA ha il seguente ciclo di vita:

FASE 1 - Attivazione della piattaforma;

FASE 2 - Configurazione della piattaforma;

FASE 3 - Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti;

FASE 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.

Quali sono le risorse di supporto ai dati?

I dati personali vengono raccolti sia mediante l'utilizzo di documenti e archivi analogici/cartacei sia attraverso l'uso di strumenti elettronico-informatici.

I dati trattati possono essere trasmessi con modalità sicure e direttamente dall'interessato tramite la piattaforma WhistleblowingPA messa a disposizione dal Titolare del Trattamento.

Il responsabile esterno del trattamento ha garantito le seguenti risorse a supporto dei dati trattati mediante la piattaforma WhistleblowingPA:

- Software diwhistleblowing professionale "GlobaLeaks"
- Infrastruttura IaaS e SaaS privata basata su tecnologie:

    1. VMWARE (virtualizzazione)
    2. Debian Linux LTS (sistema operativo)
    3. VEEAM (backup)
    4. OPNSENSE (firewall)
    5. OPENVPN (vpn)

Valutazione della sezione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità dei canali di comunicazione implementati dal Comune di Candiolo risultano conformi e sono parametrate ai dettami previsti dal Decreto Legislativo 24/2023 e alle

Linee Guida A.N.AC. adottate con delibera n. 311 del 12 luglio 2023

Valutazione della sezione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Il Trattamento dei dati tramite i canali di segnalazione interna implementati dal Titolare del trattamento si ritiene lecito in quanto effettuato sulle seguenti basi giuridiche:

- esecuzione dei compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri del RPCT **(art. 6 par. 1 lett. e)**
- adempimento agli obblighi legali discendenti dal D.lgs. 24/2023 **(art. 6 par. 1 lett. c)**

Valutazione della sezione: Accettabile

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

Si, in quanto per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati personali:

a. Nome e Cognome
b. Posizione organizzativa
c. Telefono
d. Email di ruolo dell'utente che effettua la registrazione
e. Dati relativi al Comune di Candiolo(nome, indirizzo, CF e PI).

Il software di WhistleblowingPA raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti Enti di ricerca in materia di Whistleblowing e Anticorruzione.

Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati 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.

Valutazione della sezione: Accettabile

I dati sono esatti e aggiornati?

I dati sono esatti in quanto l'inserimento e l'aggiornamento degli stessi è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata.

I dati sono altresì aggiornati in quanto non appena l'interessato modifica gli stessi all'interno della piattaforma utilizzata, questi divengono i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Valutazione della sezione: Accettabile

Qual è il periodo di conservazione dei dati?

I dati raccolti mediante i due canali di segnalazione adottati dal Titolare del Trattamento vengono conservati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati e comunque non oltre il termine previsto dal D.lgs. 24/2023.

Il portale informatico utilizzato dal Comune di Candiolo prevede una policy di Data retention impostata di default a 18 mesi, prorogabili al doppio sulle singole segnalazioni perscelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.

In ogni caso Whistleblowing Solution garantisce la piena cancellazione di tutti i dati personali trattati della piattaforma entro 15 giorni dopo la disattivazione del servizio.

Valutazione della sezione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Il segnalante e il soggetto segnalato sono informati circa le modalità di trattamento attraverso apposita informativa pubblicata sul sito web nella sezione Amministrazione Trasparente – Altri contenuti - Prevenzione corruzione, reperibile al seguente link: http://www.comune.candiolo.torino.it/servizi/Menu/dinamica.aspx?idSezione=616&idAre

a=8882&idCat=22161&ID=25883&TipoElemento=pagina

Valutazione della sezione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Non applicabile in quanto il trattamento non ha come base giuridica il consenso dell'Interessato.

Valutazione della sezione: Accettabile

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

Al fine di tutelare la riservatezza del soggetto segnalante, questi può esercitare i diritti previsti dal GDPR per iscritto rivolgendosi direttamente al RPCT.
Il segnalato viceversa, ai sensi delle Linee Guida A.N.AC. adottate con delibera n. 311 del 12 luglio 2023 non può esercitare i diritti previsti dagli art. 15-22 del GDPR.

Valutazione della sezione: Accettabile

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

Al fine di tutelare la riservatezza del soggetto segnalante, questi può esercitare i diritti previsti dal GDPR per iscritto rivolgendosi direttamente al RPCT.
Il segnalato viceversa, ai sensi delle Linee Guida A.N.AC. adottate con delibera n. 311 del 12 luglio 2023 non può esercitare i diritti previsti dagli art. 15-22 del GDPR.

Valutazione della sezione: Accettabile

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

Al fine di tutelare la riservatezza del soggetto segnalante, questi può esercitare i diritti previsti dal GDPR per iscritto rivolgendosi direttamente al RPCT.
Il segnalato viceversa, ai sensi delle Linee Guida A.N.AC. adottate con delibera n. 311 del

12 luglio 2023 non può esercitare i diritti previsti dagli art. 15-22 del GDPR.

Valutazione della sezione: Accettabile

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

Si, Whistleblowing Solution è stato formalmente nominato dal Comune di Candiolo con apposito contratto siglato il 28 agosto 2023, nel quale sono puntualmente indicate le istruzioni e gli obblighi in capo al Responsabile Esterno del trattamento.

Valutazione della sezione: Accettabile

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

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

Non viene effettuato alcun trasferimento di Dati personali degli interessati verso Paesi extra UE.

Valutazione della sezione: Accettabile

Rischi

Misure esistenti o pianificate

Crittografia

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che l'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per applicazioni di whistleblowing in collaborazione con l'Open Technology Fund di Washington.

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 a garanzia di maggiore tutela dei sistemi integralmente cifrati in condizione di fermo e in condizione di backup remoto.

Maggiori informazioni sul protocollo crittografico per il canale di segnalazione interna sono reperibili al link:

https://docs.globaleaks.org/en/main/security/EncryptionProtocol.html

Valutazione della sezione: Accettabile

Controllo degli accessi logici

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che l'accesso all'applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.
Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP

secondo standard RFC 6238.

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

Valutazione della sezione: Accettabile

Tracciabilità delle attività svolte

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che l'applicativo utilizzato implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

Valutazione della sezione: Accettabile

Archiviazione

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che l'applicativo 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.

Valutazione della sezione: Accettabile

Backup dei dati

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma

Whistleblowing, si segnala che i sistemi dell'applicativo sono soggetti a Backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

Valutazione della sezione: Accettabile

Manutenzione

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che è prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza dell'applicativo utilizzato.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Valutazione della sezione: Accettabile

Sicurezza dell'Hardware

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che 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.

Valutazione della sezione: Accettabile

Lotta contro il malware

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma

Whistleblowing PA, si segnala che il responsabile esterno ha garantito che tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware.

Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

Valutazione della sezione: Accettabile

Sicurezza dei documenti cartacei

Con riferimento al canale di segnalazione interna in forma orale tutti i dati vengono conservati all'interno di archivi (anche digitali) debitamente chiusi a chiave (anche informatica) e pertanto risultano protetti da eventuali accessi illegittimi.

Valutazione della sezione: Accettabile

Contratto con il responsabile del trattamento

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che Whistleblowing Solution è stato formalmente nominato dal Comune di Candiolo con apposito contratto siglato il 28 agosto 2023, nel quale sono puntualmente indicate le istruzioni e gli obblighi in capo al Responsabile Esterno del trattamento.

Valutazione della sezione: Accettabile

Anonimizzazione

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che nel rispetto del principio di privacy by design tutti i dispositivi utilizzati 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.

Valutazione della sezione: Accettabile

Integrare la protezione della privacy nei progetti

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che nel rispetto del principio di privacy by design tutti i dispositivi utilizzati 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.

Valutazione della sezione: Accettabile

Gestione delle politiche di tutela della privacy

L'Ente ha implementato la struttura privacy. Il Titolare ha individuato i responsabili dei singoli settori e tutti i dipendenti che trattano i dati sotto la propria autorità. Tali soggetti sono stati debitamente formati e formalmente autorizzati al trattamento ed all'accesso ai diversi sistemi informatici, archivi e/o banche dati.

È altresì presente una procedura scritta che regola tutte le operazioni necessarie per la gestione a norma di legge delle segnalazioni pervenute mediante i canali interni istituiti dal Titolare del Trattamento.

Valutazione della sezione: Accettabile

Gestione del personale

Tutto il personale è stato formato sui rischi e sulla corretta gestione dei dati personali, nonché sui maggiori rischi in ambito cybersecurity. Ciascun dipendente che tratta i dati sotto l'autorità del Titolare ha ricevuto inoltre apposita autorizzazione formale nella quale gli sono state fornite le istruzioni per una corretta gestione dei dati personali.

Valutazione della sezione: Accettabile

Gestione dei rischi

Prima dell'attivazione e dell'effettiva implementazione dei canali di segnalazione interna adottati dal Comune di Candiolo, il Titolare – anche ai sensi dell'art. 13 comma VI del D.lgs. 24/2023 – ha effettuato la presente valutazione d'impatto per valutare il rischio e le ricadute del trattamento di dati personali oggetto della presente DPIA sugli interessati e in

particolare con riferimento di dati personali del segnalante e del segnalato.

Valutazione della sezione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Il Titolare del Trattamento e i Responsabili esterni del trattamento nominati hanno adottato una procedura per la gestione degli incidenti di sicurezza (cd. data-breach).

Valutazione della sezione: Accettabile

Sicurezza dei canali informatici

Con riferimento al canale di segnalazione interna in forma scritta mediante la piattaforma Whistleblowing PA, si segnala che ogni informazione scambiata mediante l'applicativo in uso viene protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Valutazione della sezione: Accettabile

Sicurezza dei siti web

Il sito web istituzionale adibito alla segnalazione degli illeciti in forma scritta (portale WhistleblowingPA) raggiungibile al link https://comunedicandiolo.whistleblowing.it/#/ utilizza il protocollo di comunicazione sicura HTTPS.

Valutazione della sezione: Accettabile

Gestione dei terzi che accedono ai dati

Gli eventuali soggetti esterni che anche potenzialmente potrebbero avere la necessità di accedere ai dati personali racconti mediante i canali di segnalazione interna istituiti dal Comune di Candiolo per lo svolgimento di una predefinita e concordata attività (es. elaborazione statistiche storiche) e che non sono qualificabili come responsabili del trattamento, sono tenuti alla sottoscrizione di un accordo di riservatezza.

Valutazione della sezione: Accettabile

Rischi

Accesso illegittimo ai dati

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

Diffusione e divulgazione dei dati personali del segnalante e del segnalato, Perdita di riservatezza, Perdita temporanea e/o permanente dei dati trattati

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Attacchi informatici e DDoS, Comportamento umano: replica dei dati su supporto non sicuro/adatto, Comportamento umano: divulgazione involontaria delle informazioni, Comportamento umano: condotta sleale del dipendente, Fonti non umane: infezioni da virus/malware, Fonti non umane: disastri naturali, Strumenti: non adeguatezza del sistema di autenticazione, Strumenti: vulnerabilità della piattaforma WhistleblowingPA, Strumenti: trasmissione dati in maniera non sicura

Quali sono le fonti di rischio?

Comportamento Umano, Comportamento non umano, Eventi relativi agli strumenti e/o software utilizzati, Eventi relativi al contesto (social engineering e attacchi informatici)

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità delle attività svolte, Archiviazione, Backup dei dati, Manutenzione, Sicurezza dell'Hardware, Lotta contro il malware, Sicurezza dei documenti cartacei, Contratto con il responsabile del trattamento, Anonimizzazione, Integrare la protezione della privacy nei progetti, Gestione delle politiche di tutela della privacy, Gestione del personale, Gestione dei rischi, Sicurezza dei canali informatici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Sicurezza dei siti web, Gestione dei terzi che accedono ai dati

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

LIMITATA
Il rischio che vi sia una diffusione dei dati personali, con relativa perdita della riservatezza dell'identità del segnalante è da tenere in considerazione. Tuttavia, vista la realtà del Comune di Candiolo, la gravità di un eventuale accesso illegittimo può ritenersi limitata.

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

TRASCURABILE

Il Titolare del trattamento ha implementato importanti misure di sicurezza (sia organizzative sia tecniche) che permettono di abbattere la probabilità dell'evento indesiderato.

Valutazione della sezione: Accettabile

Rischi

Modifiche indesiderate dei dati

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

Errore sull'identità del segnalante o del segnalato

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

Attacchi informatici e DDoS, Comportamento umano: condotta sleale del dipendente, Comportamento umano: divulgazione involontaria delle informazioni, Comportamento umano: replica dei dati su supporto non sicuro/adatto, Fonti non umane: disastri naturali, Fonti non umane: infezioni da virus/malware, Strumenti: non adeguatezza del sistema di

autenticazione, Strumenti: trasmissione dati in maniera non sicura, Strumenti: vulnerabilità della piattaforma WhistleblowingPA.

Quali sono le fonti di rischio?

Comportamento Umano, Comportamento non umano, Eventi relativi agli strumenti e/o software utilizzati, Eventi relativi al contesto (social engineering e attacchi informatici)

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

Crittografia, Controllo degli accessi logici, Tracciabilità delle attività svolte, Archiviazione, Backup dei dati, Manutenzione, Sicurezza dell'Hardware, Lotta contro il malware, Sicurezza dei documenti cartacei, Contratto con il responsabile del trattamento, Anonimizzazione, Integrare la protezione della privacy nei progetti, Gestione delle politiche di tutela della privacy, Gestione del personale, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Sicurezza dei canali informatici, Sicurezza dei siti web, Gestione dei terzi che accedono ai dati

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

TRASCURABILE

La gravità del rischio che vi sia un errore sull'identità del segnalante è del tutto trascurabile in quanto non avrebbe particolare impatto sulla gestione della segnalazione, che ben potrebbe procedere mediante accertamenti alternativi, diversi dalle ulteriori dichiarazioni che potrebbe rendere il dichiarante; viceversa, l'errore sull'identità del segnalato – seppur più grave – non dovrebbe portare conseguenze in quanto non vi sarebbero riscontri oggettivi a supporto della segnalazione.

Pertanto, si stima la gravità del rischio complessivamente trascurabile.

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

TRASCURABILE

Il Titolare del trattamento ha implementato importanti misure di sicurezza (sia

organizzative sia tecniche) che permettono di abbattere la probabilità dell'evento indesiderato.

Valutazione della sezione: Accettabile

Rischi

Perdita di dati

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

Impossibilità di gestire le segnalazioni effettuate, Perdita di riservatezza, Perdita temporanea e/o permanente dei dati trattati, Diffusione e divulgazione dei dati personali del segnalante e del segnalato

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

Attacchi informatici e DDoS, Comportamento umano: condotta sleale del dipendente, Comportamento umano: divulgazione involontaria delle informazioni, Comportamento umano: replica dei dati su supporto non sicuro/adatto, Fonti non umane: disastri naturali, Strumenti: non adeguatezza del sistema di autenticazione, Fonti non umane: infezioni da virus/malware, Strumenti: trasmissione dati in maniera non sicura, Strumenti: vulnerabilità della piattaforma WhistleblowingPA

Quali sono le fonti di rischio?

Comportamento Umano, Comportamento non umano, Eventi relativi agli strumenti e/o software utilizzati, Eventi relativi al contesto (social engineering e attacchi informatici)

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

Crittografia, Controllo degli accessi logici, Tracciabilità delle attività svolte, Archiviazione,

Backup dei dati, Manutenzione, Sicurezza dell'Hardware, Lotta contro il malware, Sicurezza dei documenti cartacei, Anonimizzazione, Contratto con il responsabile del trattamento, Gestione dei terzi che accedono ai dati, Integrare la protezione della privacy nei progetti, Gestione delle politiche di tutela della privacy, Gestione del personale, Gestione dei rischi, Sicurezza dei canali informatici, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Sicurezza dei siti web

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

LIMITATA

Il rischio che vi sia una diffusione dei dati personali, con relativa perdita della riservatezza dell'identità del segnalante è da tenere in considerazione. Tuttavia, vista la realtà del Comune di Candiolo, la gravità di una eventuale illegittimo può ritenersi limitata.

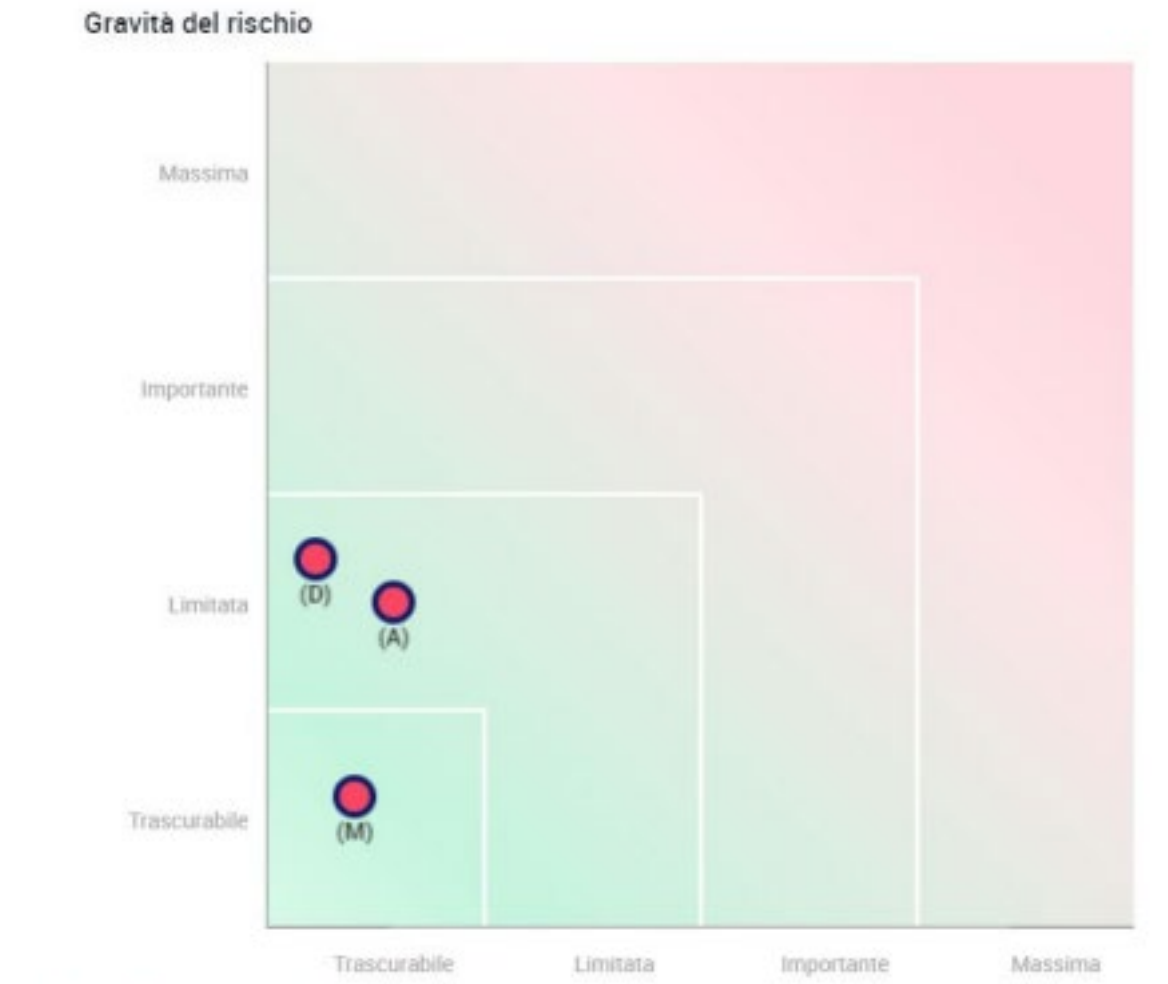
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

TRASCURABILE

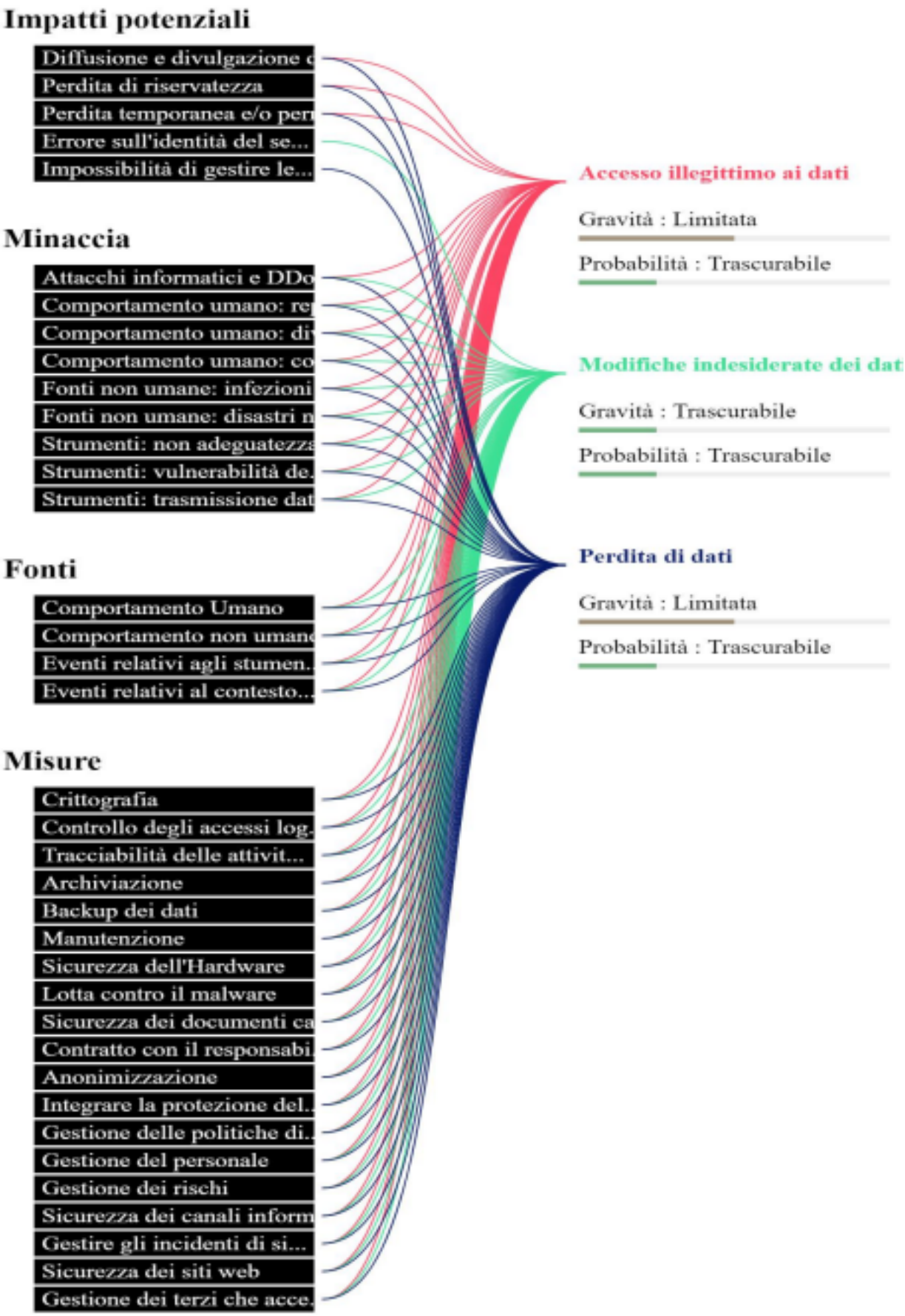
Il Titolare del trattamento ha implementato importanti misure di sicurezza (sia organizzative sia tecniche) che permettono di abbattere la probabilità dell'evento indesiderato.

Valutazione della sezione: Accettabile

Panoramica dei rischi



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


Impatti potenziali
Diffusione e divulgazione
Perdita di riservatezza
Perdita temporanea e/o per
Errore sull'identità del se...
Impossibilità di gestire le...
Minaccia
Attacchi informatici e DDo
Comportamento umano: re
Comportamento umano: di
Comportamento umano: co
Fonti non umane: infezioni
Fonti non umane: disastri n
Strumenti: non adeguatezz
Strumenti: vulnerabilità de.
Strumenti: trasmissione dat
Fonti
Comportamento Umano
Comportamento non umane
Eventi relativi agli stumen.
Eventi relativi al contesto...
Misure
Crittografia
Controllo degli accessi log.
Tracciabilità delle attivit...
Archiviazione
Backup dei dati
Manutenzione
Sicurezza dell'Hardware
Lotta contro il malware
Sicurezza dei documenti ca
Contratto con il responsabi.
Anonimizzazione
Integrare la protezione del..
Gestione delle politiche di..
Gestione del personale
Gestione dei rischi
Sicurezza dei canali inform
Gestire gli incidenti di si...
Sicurezza dei siti web
Gestione dei terzi che acce.
Accesso illegittimo ai dati
Gravità : Limitata
Probabilità : Trascurabile
Modifiche indesiderate dei dat
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Limitata
Probabilità : Trascurabile

Panoramica del piano di azione

Sulla base della presente DPIA non risulta necessario intraprendere alcuna azione correttiva.

VALUTAZIONE FINALE

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Il Titolare del trattamento ha correttamente individuato i potenziali rischi e le opportune misure di sicurezza tecniche ed organizzative per poter garantire che il trattamento oggetto della presente DPIA sia conforme al D.lgs. 24/2023, alleLinee Guida A.N.AC. adottate con delibera n. 311 del 12 luglio 2023 e a quanto previsto dal GDPR e dal Codice della Privacy.

Richiesta del parere degli interessati

È stato chiesto il parere degli interessati con nota prot. n. 15616 del 22 dicembre 2023.

Nomi degli interessati

R.S.U.

Nadia Barbero e Andrea Sarra

Posizione degli interessati

Il trattamento può essere implementato.

Pareri degli interessati

Non è pervenuto alcun riscontro.

Firmato digitalmente da
CRISTIANO MICHELA
CN = MICHELA CRISTIANO
T = Avvocato