COMUNE DI LAMEZIA TERME
Provincia di Catanzaro

DPIA
Relativa all'utilizzo di una piattaforma SW per la gestione del WHISTLEBLOWING denominata "WHISTLEBLOWING SOLUTIONS"

Approvato con Deliberazione di Giunta n. xx

INDICE

Sommario

1. DEFINIZIONI

FONTE DI RISCHIO - Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (es.; amministratore IT, utente, attaccante esterno, concorrente), o fonte non umana (acqua, materiali pericolosi, virus informatici generici) che può essere all'origine di un rischio.
GRAVITA' - La gravità rappresenta l'entità del rischio e dipende principalmente dalla natura pregiudizievole del potenziale impatto.
IMPATTO - L'impatto rappresenta il livello di gravità dell'incidente che comporta la compromissione della riservatezza, integrità e disponibilità dei trattamenti e dei dati ad essi relativi.
PROBABILITA' - La probabilità esprime la possibilità che un rischio si realizzi e dipende principalmente dal livello di vulnerabilità delle risorse di supporto quando sottoposte alle minacce e dalla capacità delle fonti di rischio di sfruttare tali vulnerabilità.
MINACCIA – La minaccia è l'evento potenziale, cagionato ovvero accidentale, che comporterebbe il danno all'interessato.
VULNERABILITA' – La vulnerabilità è l'elemento di debolezza presente all'interno del sistema informativo o informatico sfruttabile dalla minaccia per la produzione del danno.
MISURE DI SICUREZZA - Soluzioni organizzative, tecnologiche o procedurali messe in atto dal Titolare del trattamento per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al Reg. UE 679/2016.

2. CONTESTO

2.1 Panoramica del trattamento

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

Per le caratteristiche di pervasività e intrusione nella sfera dei comportamenti personali, proprie del trattamento in esame, si rende necessaria l'effettuazione della presente valutazione di impatto del trattamento.

Per le modalità di funzionamento della piattaforma WhistleblowingPA si rimanda ai documenti messi a disposizione dal fornitore all'url https://www.whistleblowing.it/documentazione-tecnica/ e che contengono:

1. Scheda Sicurezza e tecnologia;
2. Accordo di collaborazione tra Transparency International Italia e Whistleblowing Solutions IS;
3. Certificazione ISO/IEC 27001:2017.

2.2 Le figure soggettive connesse al trattamento

Titolare del Trattamento è il Comune di Lamezia Terme (CF. 00301390795) nella persona del Sindaco pro tempore. La sede legale è in via Senatore Arturo Perugini 15/C - 88046 Lamezia Terme (CZ) - Telefono: 0968.2071 Email: protocollo@comune.lamezia-terme.cz.it - PEC: protocollo@pec.comunelameziaterme.it.

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 Segretario Generale con accordo del 23.09.2021 e trasmesso nella medesima data.

Data Protection Officer è FinData Srl che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO, nella persona del dott. Mario Arcella, può essere contattato tramite il seguente indirizzo e-mail: dpo.comune.lamezia-terme@findata.it.

Il Comune di Lamezia, in qualità di Titolare del trattamento, ha designato per il trattamento dei dati personali i Dirigenti dell'Ente, ai sensi dell'art. 2, comma quaterdecies, del D.Lgs. 196/2003 e, quanto alle funzioni in materia di anticorruzione e trasparenza, il Segretario Generale quale Responsabile della prevenzione della corruzione e per la trasparenza (RPCT), il quale svolge tale attività 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.

2.3 Gli standard applicabili al trattamento

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

- Regolamento UE n. 2016/679 (GDPR);
- D.Lgs. n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.Lgs. 101/2018;
- Regolamento per la protezione dei dati personali del Comune di Lamezia Terme;
- Il D. Lgs. 10 marzo 2023, n. 24 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali.

2.4 Standard applicabili

- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID
- Certificazione CSA Star

2.5 Dati, processi e risorse di supporto

2.5.1 Tipologia dei dati trattati

Oltre ai dati comuni potrebbero essere oggetto di trattamento anche dati particolari e/o dati giudiziari.

I soggetti nei confronti dei quali possono essere effettuate le segnalazioni sono:

- il Sindaco, i Consiglieri Comunali e gli Assessori dell'Ente;
- il Segretario generale;
- i Dirigente, i dipendenti di ruolo dell'Ente e i tirocinanti;
- i componenti dei Servizi di controllo interno;
- i consulenti e i collaboratori;
- i dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso l'Ente;
- i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'Ente, nonché altri soggetti

che a vario titolo interagiscono con l'Ente stesso.

Qualora il RPCT debba avvalersi di personale dell'Ente ai fini della gestione delle pratiche di segnalazione, tale personale per tale attività è appositamente autorizzato al trattamento ai sensi dell'art. 2-quadeterdecies d.lgs. 196/2003 e, di conseguenza, il suddetto personale dovrà attenersi al rispetto delle istruzioni impartite, nonché di quelle più specifiche, connesse ai particolari trattamenti, eventualmente di volta in volta fornite dal RPCT. E' fatto salvo, in ogni caso, l'adempimento, da parte del RPCT e/o dei soggetti che per ragioni di servizio debbano conoscere l'identità del segnalante, degli obblighi di legge cui non è opponibile il diritto all'anonimato del segnalante. Con modalità tali da garantire comunque la riservatezza dell'identità del segnalante, il RPCT rende conto del numero di segnalazioni ricevute e del loro stato di avanzamento all'interno della relazione annuale di cui all'art. 1, comma 14, della legge n. 190/2012.

Il Titolare del Trattamento conserva i dati personali oggetto del trattamento denominato Whistleblowing per il periodo previsto dalla normativa vigente e, comunque, i dati personali raccolti a seguito della segnalazione sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a 18 mesi.

Il Responsabile del trattamento, all'atto della cessazione del Contratto, dovrà restituire al Comune di Lamezia Terme tutti gli eventuali dati personali di cui dovesse disporre (es. anagrafiche degli interessati, dati di contatto degli interessati) oppure, su richiesta del Titolare del trattamento provvedere alla loro distruzione, fornendone apposita attestazione, salvo eventuali esigenze di conservazione da parte del responsabile del trattamento in adempimento di obblighi normativi di cui fornirà contestuale attestazione al Comune di Lamezia Terme.

I dati personali raccolti a seguito della segnalazione, se del caso e nei limiti di legge, possono essere comunicati all'Autorità Giudiziaria, alla Corte dei Conti, al Dipartimento della Funzione Pubblica e all'ANAC.

2.5.2 Il ciclo di vita del trattamento dei dati

I dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite, delle quali sia venuto a conoscenza, commesse dai soggetti che a vario titolo interagiscono con il medesimo, vengono trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti. La gestione e la preliminare verifica sulla fondatezza delle circostanze rappresentate nella segnalazione sono affidate al RPCT che vi provvede nel rispetto dei principi di imparzialità e riservatezza effettuando ogni attività ritenuta opportuna, inclusa l'audizione personale del segnalante e di eventuali altri soggetti che possono riferire sui fatti segnalati. Qualora, all'esito di tale verifica di delibazione, si ravvisino elementi di non manifesta infondatezza del fatto segnalato, il Responsabile provvederà a trasmettere l'esito dell'accertamento per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:

- al dirigente responsabile del Servizio Risorse Umane, nonché al Responsabile dell'Area organizzativa di appartenenza dell'autore della violazione, affinché sia espletato, ove ne ricorrano i presupposti, l'esercizio dell'azione disciplinare;

- agli organi e alle strutture competenti dell'Ente affinché adottino gli eventuali ulteriori provvedimenti e/o azioni ritenuti necessari, anche a tutela dell'Ente stesso;

– se del caso, all'Autorità Giudiziaria, alla Corte dei conti, al Dipartimento della Funzione Pubblica e all'ANAC. In tali casi, nell'ambito dell'eventuale procedimento penale, l'identità del segnalante è coperta dal segreto nei modi e nei limiti previsti dall'articolo 329 del codice di procedura penale; nell'ambito del procedimento dinanzi alla Corte dei conti, l'identità del segnalante non può essere rivelata fino alla chiusura della fase istruttoria; nell'ambito del procedimento disciplinare l'identità del segnalante non può essere rivelata, ove la contestazione dell'addebito disciplinare sia fondata su accertamenti distinti e ulteriori rispetto alla segnalazione, anche se conseguenti alla stessa; in caso contrario, il segnalante può opporsi alla rivelazione della propria identità, di conseguenza il procedimento deve essere archiviato.

–

Pertanto, i dati non verranno diffusi, ma comunicati secondo le previsioni della normativa vigente.

Non vi è trasferimento all'estero dei dati personali trattati.

L'interessato può esercitare i diritti di cui agli artt. 15 e segg. del GDPR utilizzando i dati di contatto del Titolare indicati al punto 2.2 di questo documento oppure facendo riferimento al Responsabile della Protezione dei dati - DPO dpo.comune.lamezia-terme@findata.it.

2.5.3 Le risorse di supporto ai dati

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

1. PRINCIPI FONDAMENTALI

3.1 Proporzionalità e necessità

3.1.1 Gli scopi del trattamento dei dati

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

3.1.2 Le basi legali che rendono lecito il trattamento

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

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

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

3.1.3 Adeguatezza, pertinenza e limiti: la minimizzazione dei dati

In applicazione del principio della pertinenza, le segnalazioni raccolte e l'identità del segnalante vengono raccolti in base a quanto rappresentato dal whistleblower. Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI). Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di

navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

3.1.4 Esattezza ed aggiornamento dei dati

L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento. Inoltre, Il Comune di Lamezia Terme adotta tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

3.1.5 Periodo di conservazione dei dati

In conformità all'art. 14 del d.lgs. 24/2023, il Comune di Lamezia Terme conserva i dati relativi alle segnalazioni per il tempo necessario al trattamento della segnalazione e comunque non oltre 5 anni a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. Come indicato in precedenza, il Responsabile del trattamento, all'atto della cessazione del Contratto, dovrà restituire al Comune di Lamezia tutti gli eventuali dati personali di cui dovesse disporre o, in alternativa, su richiesta del Titolare del trattamento provvedere alla loro distruzione, fornendone apposita attestazione, salvo eventuali esigenze di conservazione in adempimento di obblighi normativi gravanti sullo stesso Responsabile del trattamento, di cui fornirà contestuale attestazione al Comune di Lamezia Terme.

Quest'ultimo conserva i dati personali oggetto del trattamento in questione per il periodo previsto dalla normativa vigente e, comunque, i dati personali raccolti a seguito della segnalazione sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore a 18 mesi.

3.2 Misure a tutela dei diritti degli interessati

3.2.1 L'informativa agli interessati

Gli interessati al trattamento sono informati tramite un'informativa liberamente consultabile alla sezione "Amministrazione Trasparente" del sito istituzionale del Comune di Lamezia Terme o tramite la consegna cartacea dell'informativa in occasione dell'incontro con il RPCT.

3.2.2 Modalità di ottenimento del consenso

Dato atto che per consenso dell'interessato si intende *qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento,* qualora la contestazione sia fondata, in tutto o in parte, e la conoscenza dell'identità del segnalante sia indispensabile per la difesa dell'incolpato, la segnalazione sarà utilizzabile ai fini del procedimento disciplinare solo in presenza di consenso del segnalante alla rivelazione della sua identità; in caso contrario il procedimento dovrà essere archiviato.

3.2.3 Esercizio del diritto di accesso dei dati

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

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

A tal fine possono essere utilizzati i dati di contatto che il Titolare ha pubblicato all'interno dell'Informativa Privacy per il Whistleblowing e sul sito istituzionale.

3.2.4 Esercizio dei diritti di rettifica e cancellazione

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

A tal fine possono essere utilizzati i dati di contatto che il Titolare ha pubblicato all'interno dell'Informativa Privacy per il Whistleblowing e sul sito istituzionale. Il Titolare, allo scopo di agevolare l'esercizio dei diritti degli interessati ha anche predisposto e pubblicato sul sito istituzionale apposito modello da utilizzare.

3.2.5 Esercizio dei diritti di limitazione e opposizione

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

A tal fine possono essere utilizzati i dati di contatto che il Titolare ha pubblicato all'interno dell'Informativa Privacy per il Whistleblowing e sul sito istituzionale. Il Titolare, allo scopo di agevolare l'esercizio dei diritti degli interessati ha anche predisposto e pubblicato sul sito istituzionale apposito modello da utilizzare.

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

Gli obblighi del Responsabile esterno sono definiti tramite il contratto sottoscritto con il Titolare del Trattamento e la relativa nomina di responsabile esterno. Tali obblighi riguardano, oltre la Whistleblowing Solutions in qualità di Responsabile del trattamento, i seguenti soggetti: Seeweb Srl in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions e Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions. Non è previsto che i dati vengano trasferiti al di fuori dello spazio economico europeo.

2. RISCHI

4.1 Misure di prevenzione esistenti o pianificate

4.1.1 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.

4.1.2 Controllo degli accessi logici

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali. Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password. Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238. Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

4.1.3 Tracciabilità

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

4.1.4 Archiviazione

L'applicativo GlobaLeaks implementa un database SQLite integrato acceduto tramite ORM. Le configurazioni effettuate sono tali da garantire elevate garanzie di sicurezza grazie al completo controllo da parte dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

4.1.5 Controlli sulle vulnerabilità

L'applicativo GlobaLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza indipendenti di ampio respiro su base almeno annuale e tutti i report vengono pubblicati per finalità di peer review. A questi si aggiunge la peer review indipendente realizzata dalla crescente comunità di stakeholder composta da un crescente numero di società quotate, fornitori e utilizzatori istituzionali che su base regolare commissionano audit indipendenti che vengono forniti al progetto privatamente. Audit di sicurezza: https://docs.globaleaks.org/en/main/security/PenetrationTests.html.

4.1.6 Backup

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

4.1.7 Manutenzione

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza. Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti. Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

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

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

4.1.10 Gestione incidenti di sicurezza e violazioni dei dati personali
Sia il Comune di Lamezia Terme che Whistleblowing Solutions, hanno definito delle procedure per la gestione delle violazioni dei dati personali.

4.1.11 Lotta contro i malware
Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware. Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

4.1.12 Minimizzazione dei dati e anonimato
Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

4.1.13 Misure organizzative
GESTIONE DEL PERSONALE: Il Titolare del trattamento ha provveduto e provvede costantemente alla formazione dei soggetti designati/autorizzati al trattamento dei dati personali. I soggetti designati/autorizzati al trattamento dei dati sono nominati con specifici atti, come da Regolamento comunale e sono istruiti e formati sul corretto trattamento.

GESTIONE DEI TERZI CHE ACCEDONO AI DATI: L'accesso ai dati da parte di terzi è legittimato da contratti o convenzioni. Gli accessi da parte dei terzi sono tracciati ed autorizzati dai sistemi informativi comunali con utenze personali e a scadenza.

VIGILANZA SULLA PROTEZIONE DEI DATI: Il Titolare del trattamento svolge una costante attività di verifica dei trattamenti effettuati e se necessario provvede all'aggiornamento del Registro delle attività di trattamento, delle Valutazioni di impatto, delle informative.

3. RISCHI MAPPATI

5.1 ACCESSO ILLEGITTIMO AI DATI

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Azioni ritorsive nei confronti del segnalante, dei colleghi di lavoro o delle persone che sono legate ad esso da uno stabile legame affettivo o di parentela entro il quarto grado e pregiudizio alla sua reputazione.

Quali sono le principali minacce che potrebbero concretizzare il rischio?
accesso non autorizzato ai sistemi del Comune per operazioni non consentite/non autorizzate, azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

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

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

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

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

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

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

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

5.2 MODIFICHE INDESIDERATE DEI DATI

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

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

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

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

Quali sono le fonti di rischio?

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

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

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

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

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

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

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

5.3 PERDITA DI DATI

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

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

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

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

Quali sono le fonti di rischio?

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

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

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

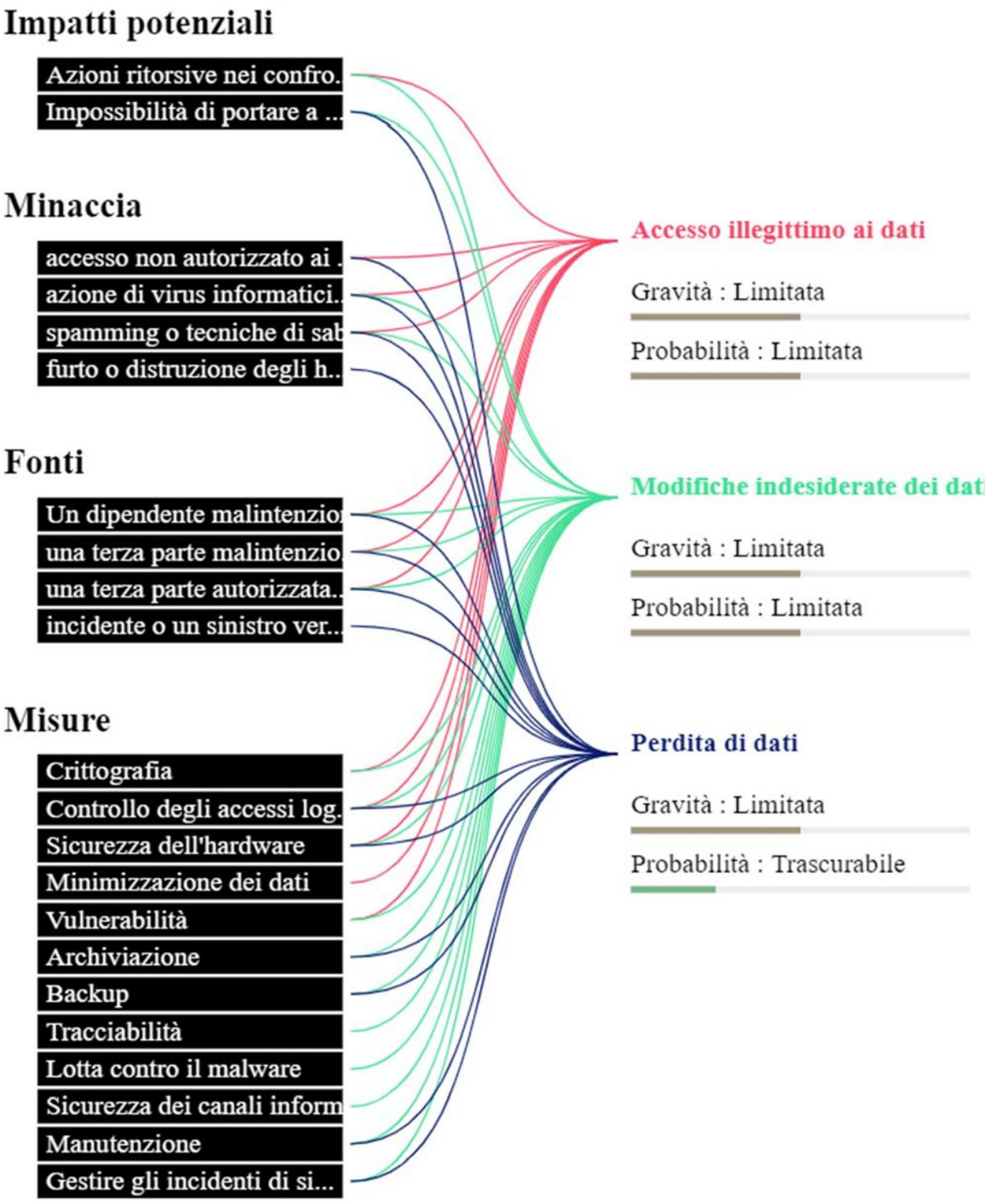
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

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

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

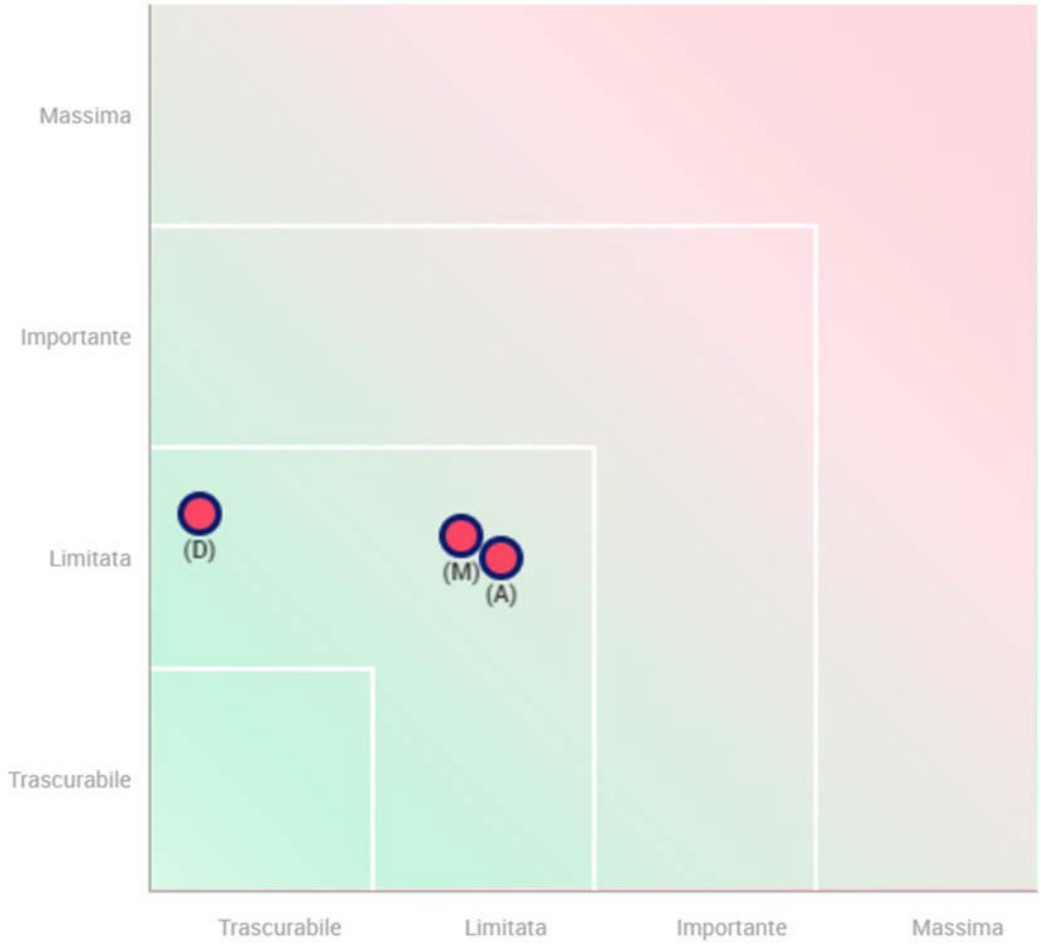
Trascurabile, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

6. Panoramica dei rischi



7. MAPPATURA DEL RISCHIO

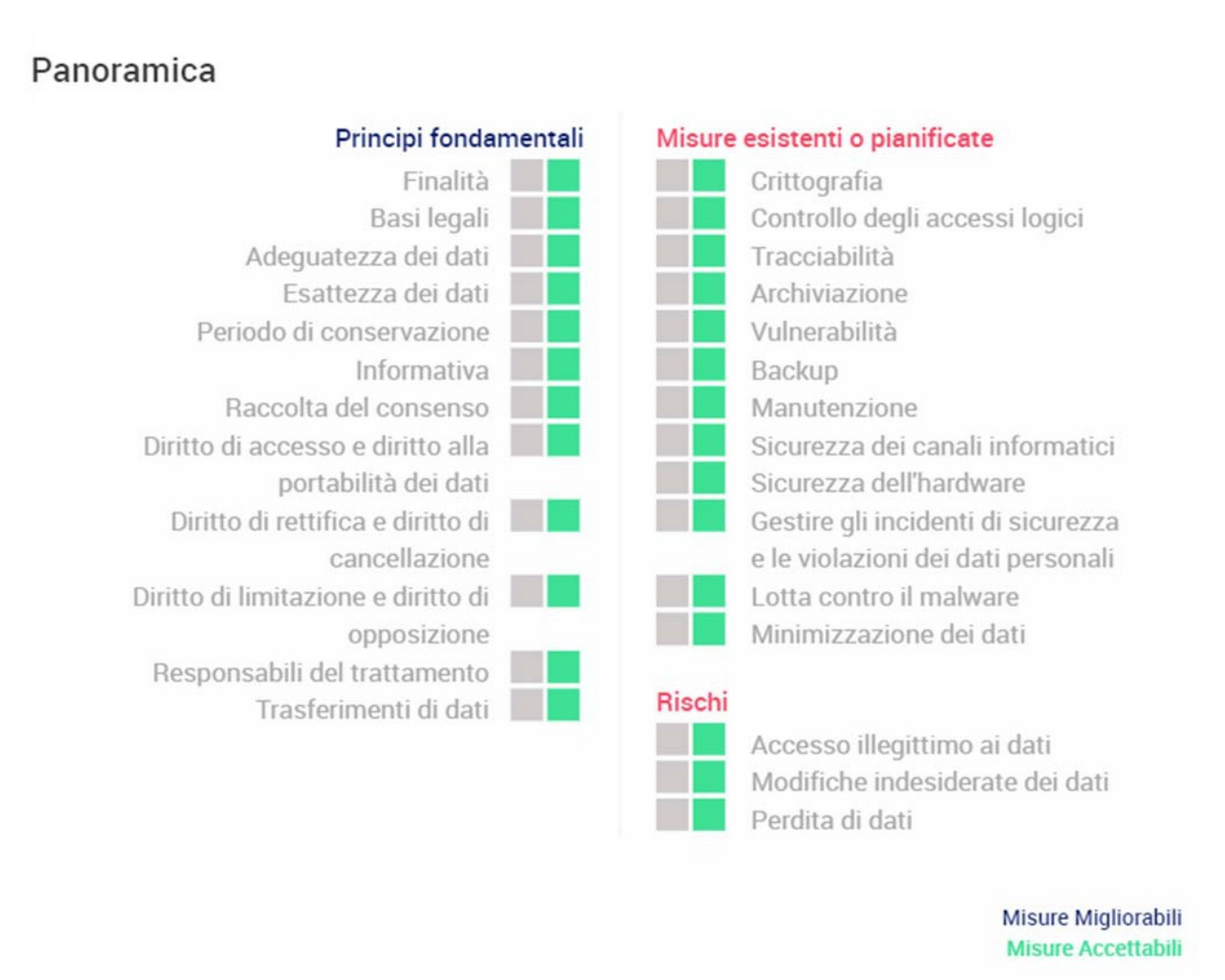
Gravità del rischio



Probabilità del rischio

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

8. PIANO D'AZIONE DEL RISCHIO



9. VALIDAZIONE

Titolare del Trattamento – Comune di Lamezia Terme
Segreteria Generale del Comune di Lamezia Terme

Parere del DPO: Parere POSITIVO, come da Prot. Int. n. CZ_LA_2023_21-FND.