Provincia di Prato
documento di Valutazione di impatto sulla protezione dei dati
(DPIA - *DATA PROTECTION IMPACT ASSESSMENT*)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "possa presentare un rischio elevato".

Titolare del trattamento:
PROVINCIA DI PRATO

Legale rappresentante:
Simone Calamai

Responsabile della protezione dei dati (RPD/DPO):
Avv. Nadia Corà

Sede:
Via Ricasoli, n. 25, Prato (PO)

Data:
29/02/2024

DPIA per l’utilizzo della piattaforma WhistleblowingIT

PANORAMICA DEL TRATTAMENTO

Descrizione del contesto in cui avviene il trattamento

La nuova disciplina del whistleblowing è normata dal d.lgs. n. 24/2023 *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* (GU Serie Generale n. 63 del 15/03/2023), decreto entrato in vigore lo scorso 30 marzo 2023 e produttivo di effetti a decorrere dal 15 luglio 2023.

Le principali novità della normativa di whistleblowing sono:

a) la specificazione dell'ambito soggettivo con riferimento agli enti di diritto pubblico, di quelli di diritto privato e l’estensione del novero di questi ultimi;

b) l’ampliamento dei soggetti che possono essere protetti per le segnalazioni, denunce o divulgazioni pubbliche;

c) l’espansione di ciò che è considerato violazione rilevante ai fini della protezione;

d) la disciplina di tre canali di segnalazione: interno, esterno e divulgazione pubblica;

e) la disciplina dettagliata degli obblighi di riservatezza e del trattamento dei dati personali;

f) i chiarimenti su che cosa si intende per ritorsione e ampliamento della relativa casistica;

g) l’introduzione di apposite misure di sostegno per le persone segnalanti e il coinvolgimento a tal fine degli enti del Terzo settore;

h) la tutela anche durante il periodo di prova e anteriormente o successivamente alla costituzione del rapporto di lavoro;

i) la tutela dei soggetti diversi dal segnalante che potrebbero essere destinatari di ritorsioni in ragione del ruolo assunto nell'ambito del processo di segnalazione;

l) la revisione della disciplina delle sanzioni applicabili da ANAC.

La piattaforma WhistleblowingIT nasce nel 2018 con il nome di WhistleblowingPA grazie alla volontà di Transparency International Italia e di Whistleblowing Solutions Impresa Sociale di offrire a tutte le Pubbliche Amministrazioni un software informatico gratuito per dialogare con i segnalanti, grazie a modalità che garantiscono sicurezza e anonimato.

Dal 2023 l’iniziativa cambia nome e diventa *WhistleblowingIT* per abbracciare anche nella sua identità le diverse componenti di questo progetto che sono cresciute negli anni. Infatti, a seguito delle sempre maggiori richieste ricevute da enti diversi dalle PA, Transparency International Italia e Whistleblowing Solutions hanno deciso di andare incontro alle esigenze di società in controllo pubblico, di società private e di enti e organizzazioni che vogliono dotarsi di sistemi di segnalazioni di illeciti, grazie a nuove soluzioni standard e personalizzate. Tutto ciò continuando a mantenere al cuore dell’iniziativa il suo scopo sociale che permette di servire tutte le pubbliche amministrazioni gratuitamente, un numero in costante crescita.

Il progetto mette a disposizione delle piattaforme informatiche realizzate grazie al software GlobaLeaks, l’unica soluzione di whistleblowing digitale libera e open source. Tutte le piattaforme sono conformi alla legge sulla tutela dei segnalanti e il loro mantenimento e aggiornamento sono

sempre garantiti e non richiedono interventi tecnici da parte di soggetti interni o esterni agli enti o alle organizzazioni. Inoltre, WhistleblowingPA è un servizio qualificato ACN.

Soggetti coinvolti nel trattamento

- Titolare del trattamento: Provincia di Prato
- Responsabile del trattamento (per la fornitura e la gestione del sistema di whistleblowing): Whistleblowing Solutions
- Sub-Responsabile del trattamento: Seeweb (nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura IaaS)
- Sub-Responsabile del trattamento: Transaparency International Italia (nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing)

Standard applicabili al trattamento

- 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, PROCESSI E RISORSE DI SUPPORTO

Tipologia di dati trattati

- 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 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 di supporto ai dati

Sono utilizzate le seguenti risorse a supporto dell'attività di trattamento:

- software di whistleblowing professionale GlobaLeaks;
- infrastruttura IaaS e SaaS privata basata su VMWARE (virtualizzazione), Debian Linux LTS (sistema operativo), VEEAM (backup), OPNSENSE (firewall), OPENVPN (vpn).

PRINCIPI FONDANTI IL TRATTAMENTO

Scopo del trattamento:
L'attività di trattamento è specifica, esplicita e legittima in quanto aderente a quanto previsto dal D.Lgs 24/2023. Le finalità sono esplicitate anche nell'informativa scaricabile dalla piattaforma di gestione delle segnalazioni e sul sito internet della Provincia.

Basi legali che rendono lecito il trattamento:
La base giuridica del trattamento è l'obbligo di legge previsto dal D.Lgs 24/2023.

Minimizzazione dei dati
I dati raccolti sono adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per le quali i dati sono trattati (c.d. minimizzazione).

Aggiornamento e correttezza 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.

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 per un periodo massimo di 5 anni di conservazione a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione, come previsto dall'art. 14 del D.lgs 24/2023. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte.

Informazioni sul trattamento agli interessati
Gli interessati sono informati del trattamento attraverso:
- l'informativa privacy raggiungibile dalla piattaforma e dal sito internet della Provincia;
- la pubblicazione di una news sul sito internet istituzionale;
- la pubblicazione della notizia sulla intranet aziendale;
- tramite il PIAO 2024-2026 di prossima approvazione.

ESERCIZIO DEI DIRITTI DA PARTE DEGLI INTERESSATI

Diritti di accesso e di portabilità dei dati
Gli interessati sono informati che possono contattare il titolare del trattamento attraverso i punti di contatto del responsabile protezione dati.

Diritti di rettifica e di cancellazione
Gli interessati sono informati che possono contattare il titolare del trattamento attraverso i punti di contatto del responsabile protezione dati.

Diritti di limitazione e di opposizione
Gli interessati sono informati che possono contattare il titolare del trattamento attraverso i punti di contatto del responsabile protezione dati.

RESPONSABILI ESTERNI AL TRATTAMENTO

I rapporti con il responsabile esterno al trattamento, Whistleblowing Solutions, sono definiti mediante apposito contratto e nomina ex art. 28 GDPR.
In particolare 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

LUOGO DI CONSERVAZIONE DEI DATI ED EVENTUALI TRASFERIMENTI

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.

GESTIONE DEI RISCHI DERIVANTI DAL TRATTAMENTO

MISURE TECNICHE ED ORGANIZZATIVE ESISTENTI

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.

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

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 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.

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.

Contratto con il responsabile del trattamento
è stato stipulato un contratto ex art. 28 GDPR con il responsabile del trattamento

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.

TIPOLOGIE DI RISCHIO DERIVANTI DAL TRATTAMENTO

a) Accesso illegittimo ai dati
Possibili impatti sugli interessati se il rischio si dovesse concretizzare
Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative
Principali minacce che potrebbero concretizzare il rischio
Accesso non autorizzato ai sistemi della Provincia per operazioni non consentite/non autorizzate, Azione di virus informatici o di programmi suscettibili di recare danno, Spamming, Tecniche di sabotaggio
fFonti di rischio
Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale), Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker), Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)
Misure, fra quelle individuate, che contribuiscono a mitigare il rischio
Crittografia, Controllo degli accessi logici, Tracciabilità, Sicurezza dei canali informatici, Lotta contro il malware, Sicurezza dell'hardware, Manutenzione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Vulnerabilità

_____
Stima della gravità del rischio alla luce degli impatti potenziali e delle misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza contro l'accesso illegittimo ai dati.
Stima probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza contro l'accesso illegittimo ai dati.

b) Modifiche indesiderate dei dati
Impatti sugli interessati se il rischio si dovesse concretizzare.
Disagio, Diffusione indesiderata dei propri dati, Consultazione dei propri da parte di personale non autorizzato, Ricatto economico, Problematiche di natura giuslavoristica e contrattuale, Mobbing, Discriminazioni lavorative
Principali minacce che potrebbero consentire la concretizzazione del rischio.
Azione di virus informatici o di programmi suscettibili di recare danno, Spamming, Tecniche di sabotaggio

Fonti di rischio.
Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale), Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker), Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)

Misure, fra quelle individuate, che contribuiscono a mitigare il rischio.
Controllo degli accessi logici, Tracciabilità, Vulnerabilità, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro il malware

---

Stima della gravità del rischio alla luce degli impatti potenziali e delle misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza per quanto riguarda modifiche indesiderate ai dati.

Stima probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza per quanto riguarda modifiche indesiderate ai dati.

c) Perdita di dati

Impatti principali sugli interessati se il rischio dovesse concretizzarsi
Discriminazioni lavorative, problematiche di natura giuslavoristica e contrattuale, disagio.

Minacce che potrebbero consentire la materializzazione del rischio.
Accesso non autorizzato ai sistemi della Provincia per operazioni non consentite/non autorizzate, Azione di virus informatici o di programmi suscettibili di recare danno, Spamming, Tecniche di sabotaggio

Fonti di rischio.
Fonti umane interne (es. dipendenti, collaboratori, la cui condotta può essere accidentale o intenzionale), Fonti umane esterne (es. fornitori la cui condotta può essere accidentale o intenzionale, attaccanti e hacker), Fonti non umane (es. allagamenti, materiali pericolosi o virus informatici generici)

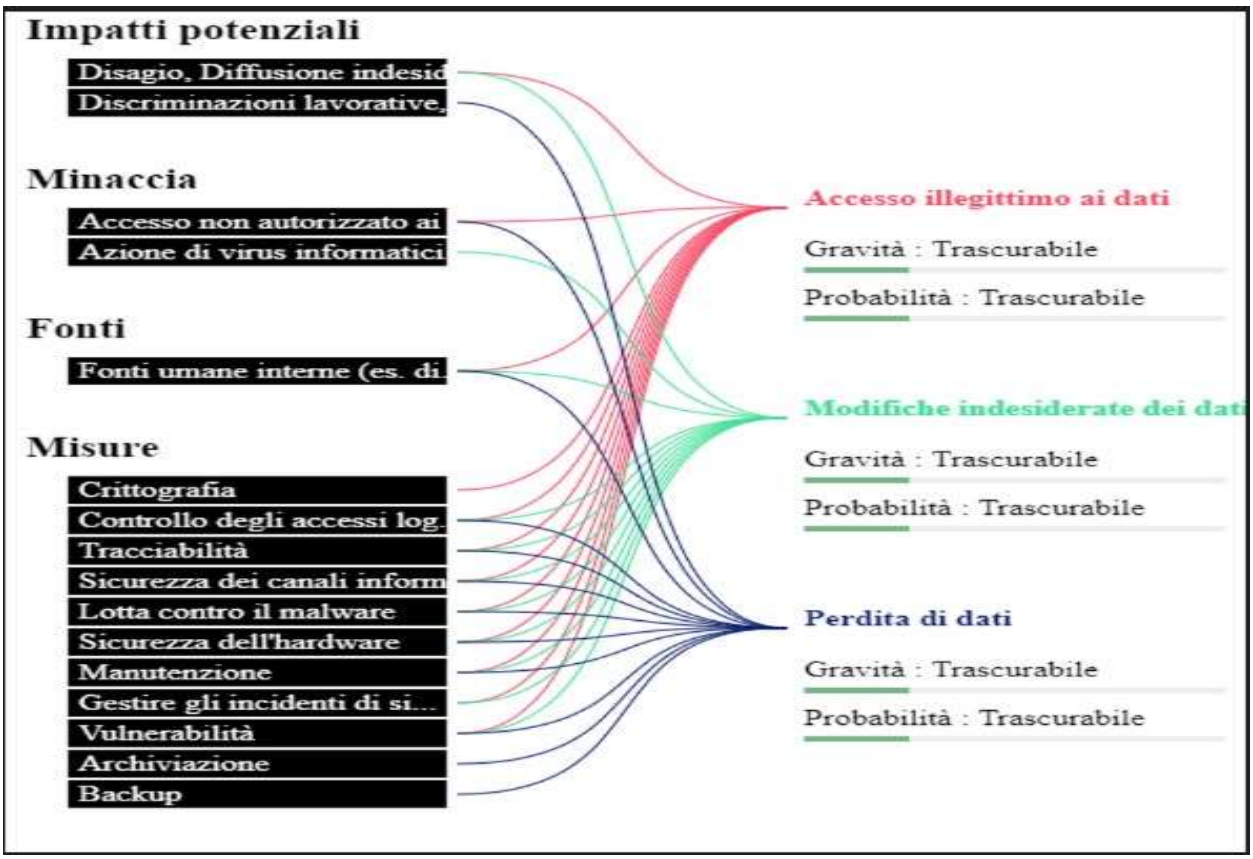
Misure, fra quelle individuate, che contribuiscono a mitigare il rischio.
Controllo degli accessi logici, Tracciabilità, Archiviazione, Vulnerabilità, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Lotta contro il malware

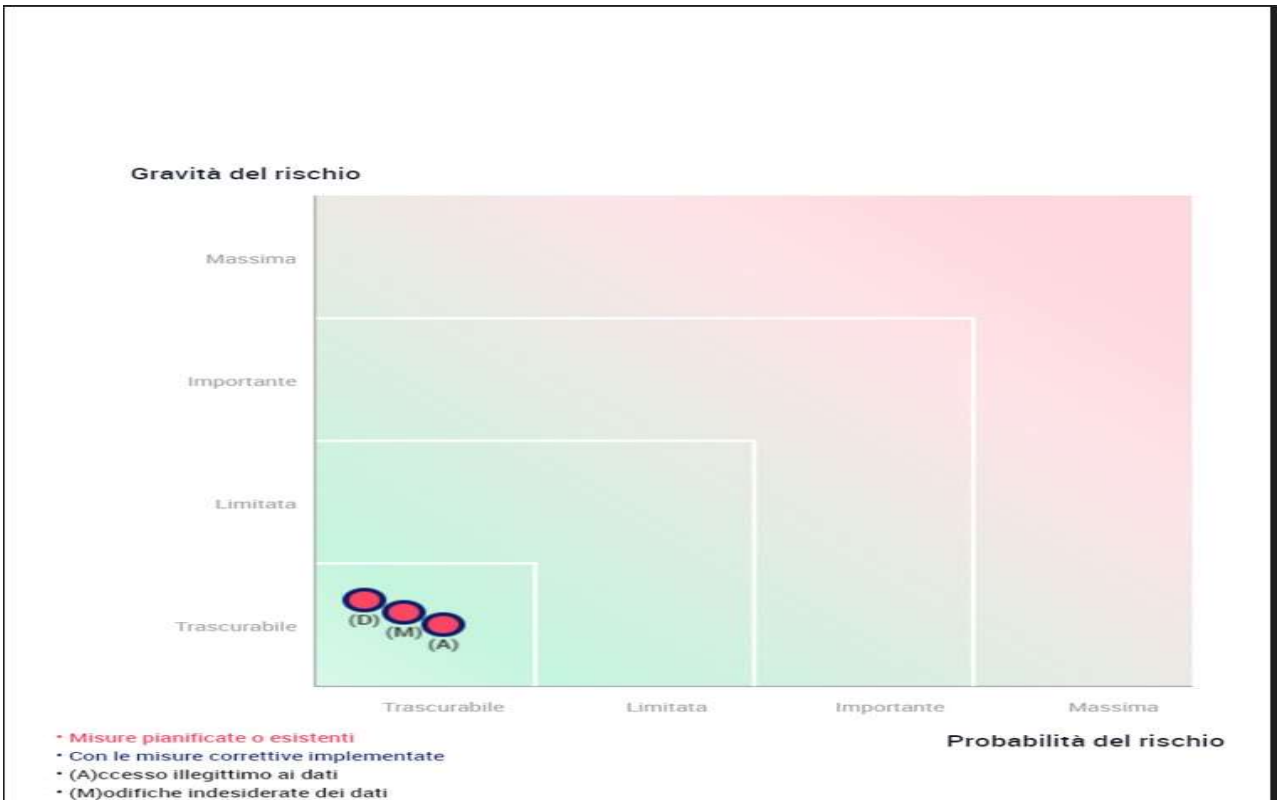
---

Stima della gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza contro la perdita di dati.

Stima della probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate
Trascurabile. Le misure messe in atto garantiscono un buon livello di sicurezza contro la perdita di dati.

PANORAMICA DEI RISCHI IN SEGUITO ALL'APPLICAZIONE DELLE MISURE





CONCLUSIONI

Alla luce dell'analisi fin qui condotta, si ritiene che le descritte contromisure adottate in considerazione di un rischio trascurabile, possano ragionevolmente renderlo gestibilite da parte del Titolare.

In quest’ottica, si ritiene quindi superflua, salvo parere contrario del DPO, la consultazione preventiva dell’Autorità Garante ai sensi e per gli effetti dell’art. 36 del Regolamento UE 679/2016.

Il Presidente della Provincia
(titolare del trattamento)
Simone Calamai