DPIA – Trattamento dati Segnalazione illeciti

DPO e Titolare del trattamento/Delegato

Nome del DPO/RPD

Igino Addari

Parere del DPO/RPD

Trattamento implementabile in quanto conforme al GDPR 2016/679

Richiesta del parere del Titolare del trattamento/Delegato

È stato chiesto il parere del Titolare del trattamento/Delegato.

Nomi del Titolare del trattamento/Delegato

Gianfranco De Massis – Comune di Elice

Posizione del Titolare del trattamento/Delegato

Il trattamento può essere implementato.

Pareri del Titolare del trattamento/Delegato

Trattamento implementabile in quanto conforme al GDPR 2016/679

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Attività relativa alla segnalazione di illeciti, whistleblowing, svolta con software i cui dati tecnici e funzionali sono dichiarati dal fornitore.

Quali sono le responsabilità connesse al trattamento?

Titolare del Trattamento: Comune di Elice

Responsabile del trattamento: **Whistleblowing Solutions** fornitore e gestore del sistema di segnalazione degli illeciti - whistleblowing

Sub-Responsabile del trattamento: **Seeweb** per la gestione dell'infrastruttura (Iaas)

Sub-Responsabile del trattamento: **Transparency International Italia per la collaborazione nella gestione del sistema di whistleblowing**

Ci sono standard applicabili al trattamento?

Linee guida in materia di tutela del dipendente pubblico che segnala illeciti (c.d. whistleblower)" emanate da ANAC.
Come da indicazioni fornite dal fornitore del software, conformità normativa a:

- D.Lgs. n. 24/2023 o altra normativa nazionale in caso di entità giuridiche con sede in altro Paese.
- DIRETTIVA (UE) 2019/1937 (WHISTLEBLOWING)
- GENERAL DATA PROTECTION REGULATION - 2016/679 (GDPR)

Il servizio erogato adotta misure progettate in aderenza allo standard internazionale ISO37002:2021 in materia di gestione dei processi di whistleblowing.

Il Responsabile adotta un modello di gestione integrata dei propri processi di fornitura SaaS certificato:

- ISO/IEC 27001:2022
- ISO/IEC 27017:2015
- ISO/IEC 27018:2019
- ISO 9001:2015
- CSA STAR Level 1
- ACN

Valutazione: Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?

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.

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

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 par te 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.

Quali sono le risorse di supporto ai dati?

Come da indicazioni fornite dal fornitore del software, 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)

Valutazione: Accettabile

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Le finalità del trattamento sono specifiche esplicite e legittime in forza di legge.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Dlgs n. 24 del 10 marzo 2023; Linee Guida ANAC delibera n.311 del 12/07/2023; Legge n. 179 del 30 novembre 2017; legge 6 novembre 2012, n. 190 art. 1, c. 51.

Valutazione: Accettabile

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

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 impor tanti 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 di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità di accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.
Al fine di consentire la possibilità di segnalazioni orali e al contempo tutelare l'anonimato e la confidenzialità, il sistema applica avanzate tecniche di "vocoding" (atte a evitare di raccogliere il timbro vocale) e "pitch shifting" (atte a variare il tono della voce in modo casuale) capaci di offrire elevate caratteristiche di anonimizzazione al passo con la ricerca nello specifico contesto d'uso. Tali tecniche permettono ai riceventi di ascoltare la registrazione senza essere in condizione di identificare la voce direttamente e rendendo altamente inefficaci tecniche moderne di de-anonimizzazione. Nonostante la registrazione venga protetta sotto questo profilo e venga mantenuta in forma alla pari di ogni allegato della segnalazione, per l'ascolto è indicato l'uso di cuffie per limitare l'esposizione del contenuto del messaggio.

Valutazione: Accettabile

I dati sono esatti e aggiornati?

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.

Valutazione: Accettabile

Qual è il periodo di conservazione dei dati?

Policy di data retention di default delle segnalazioni di 12 mesi, con cancellazione automatica sicura delle segnalazioni che raggiungono la data di scadenza. Il gestore può anticipare la scadenza delle segnalazioni fino a 3 mesi dalla data dell'operazione e può prorogare la scadenza delle segnalazioni per il tempo ritenuto congruo al trattamento dei dati.
Anticipazioni e proroghe delle scadenze possono essere fatte dal gestore più volte.
Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

Valutazione: Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

La segnalazione è coperta dal segreto nei modi e nei termini di cui all'articolo 329 del codice di procedura penale. La segnalazione è sottratta all'accesso previsto dagli articoli 22 e seguenti della legge 7 agosto 1990, n. 241, e successive modificazioni.
L'informativa privacy per la segnalazione di illeciti è presente in calce alla pagina descrittiva del servizio di segnalazione illeciti (https://www.comune.elice.pe.it/whistleblowing/).

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Nel passo conclusivo della segnalazione, il segnalante deve accettare per presa visione la seguente dicitura: "Per conoscere le modalità di gestione delle segnalazioni, della trasmissione delle informazioni, del trattamento e della conservazione dei dati personali ti invitiamo a visionare l'apposita procedura sul sito dell'amministrazione, nonché la specifica informativa privacy."

Valutazione: Accettabile

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

Come previsto nell'informativa privacy sopra citata, gli interessati hanno il diritto di ottenere dall'Ente, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza al Titolare del trattamento o al Responsabile della Protezione dei dati personali può essere presentata all'indirizzo segretario@comune.elice.pe.it

Valutazione: Accettabile

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

Come previsto nell'informativa privacy sopra citata, gli interessati hanno il diritto di ottenere dall'Ente, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza al Titolare del trattamento o al Responsabile della Protezione dei dati personali può essere presentata all'indirizzo segretario@comune.elice.pe.it

Valutazione: Accettabile

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

Come previsto nell'informativa privacy sopra citata, gli interessati hanno il diritto di ottenere dall'Ente, nei casi previsti, l'accesso ai propri dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento L'apposita istanza al Titolare del trattamento o al Responsabile della Protezione dei dati personali può essere presentata all'indirizzo segretario@comune.elice.pe.it

Valutazione: Accettabile

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

Sono definiti a norma del Dlgs n. 24 del 10 marzo 2023 e dalle Linee Guida ANAC delibera n.311 del 12/07/2023.
Inoltre, 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.

Valutazione: 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 esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

Valutazione: Accettabile

Rischi

Misure esistenti o pianificate

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.

Controllo degli accessi fisici

Utente e password per la gestione informatizzata.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

1. Informare immediatamente il Titolare del trattamento dei dati personali (Legale rappresentante) e il Responsabile per la Prevenzione della Corruzione e Trasparenza RPCT;
2. Rimettere una relazione dettagliata al Titolare del trattamento dei dati personali;
3. Redigere il tool di autovalutazione messa a disposizione dal Garante che aiuta a determinare se e in quale caso inviare una notifica di violazione dei dati personali. Il tool è raggiungibile al seguente URL: https://servizi.gpdp.it/databreach/s/self-assessment ;
4. Se dalla compilazione del tool di autovalutazione emerge la necessita di inviare la notifica, il titolare del Trattamento deve eseguire, entro 48/72 ore, la notifica al Garante;
5. Valutare, in base alla gravità, l'eventuale successiva comunicazione della violazione all'interessato.

Procedura cartacea

Non prevista.

Anonimizzazione

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.

Partizionamento

Non previsto.

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.
Ogni log di audit viene mantenuto per un periodo massimo di 5 anni, fatto salvo il caso specifico dei log pertinenti le segnalazioni che vengono mantenuti per tutto il tempo di conservazione delle stesse.
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 par te dell'applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

Sicurezza dei documenti cartacei

Non prevista.

Minimizzazione dei dati

Limitazione dei dati trattati a quelli indispensabili ai fini della procedura attivata a norma ANAC.

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.

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.

Gestione postazioni

Accesso riservato al RPCT.

Sicurezza dei siti web

Sicurezza https su piattaforma riservata.

Backup

I sistemi sono soggetti a backup remoto con frequenza di 8 ore e policy di data retention di 7 giorni necessari per finalità di disaster recovery garantendo dunque una RPO di 8 ore.

Manutenzione

È 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.

Contratto con il responsabile del trattamento

Si. Nomina del fornitore del software.

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.

Prevenzione delle fonti di rischio

Rispetto delle Linee guida dell'ANAC.

Protezione contro fonti di rischio non umane

Accessibilità riservata a RPCT.

Politica di tutela della privacy

Il Titolare del trattamento nomina DPO, forma i soggetti autorizzati, nomina responsabili del trattamento dei dati personali esterni di comprovata esperienza.

Gestione delle politiche di tutela della privacy

Registro delle attività di trattamento, attuazione del principio di accountability per dimostrare l'assolvimento degli adempimenti previsti dal GDPR.

Gestione dei rischi

Accesso controllato, crittografia, minimizzazione del trattamento dei dati personali.

Integrare la protezione della privacy nei progetti

Attuazione privacy by default. Informativa privacy al segnalante, che dichiara i suoi dati, di cui prendere visione all'accesso.

Gestione del personale

Formazione e istruzioni GDPR dei soggetti autorizzati al trattamento dei dati personali.

Gestione dei terzi che accedono ai dati

Eventuale accesso o coinvolgimento di terzi autorizzato dal RPCT.

Vigilanza sulla protezione dei dati

Audit periodici.

Rischi

Accesso illegittimo ai dati

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

Rischio di inquinamento delle prove.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Identificazione del segnalante.

Quali sono le fonti di rischio? Fonti umane interne.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi fisici. Crittografia. Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

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

Gravità del rischio importante.

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

Limitata, Probabilità del rischio limitata.

Modifiche indesiderate dei dati

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

Impatto sul segreto istruttorio.

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

Mancato rispetto delle procedure.

Quali sono le fonti di rischio?

Fonti umane interne.

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

Crittografia. Controllo degli accessi fisici.

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

Gravità importante.

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

Limitata.

Rischi

Perdita di dati

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

Blocco indagini, ritorsioni.

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

Minacce umane interne, trattamenti cartacei.

Quali sono le fonti di rischio?

Fonti umane interne, errore.

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

Crittografia, Controllo degli accessi fisici.

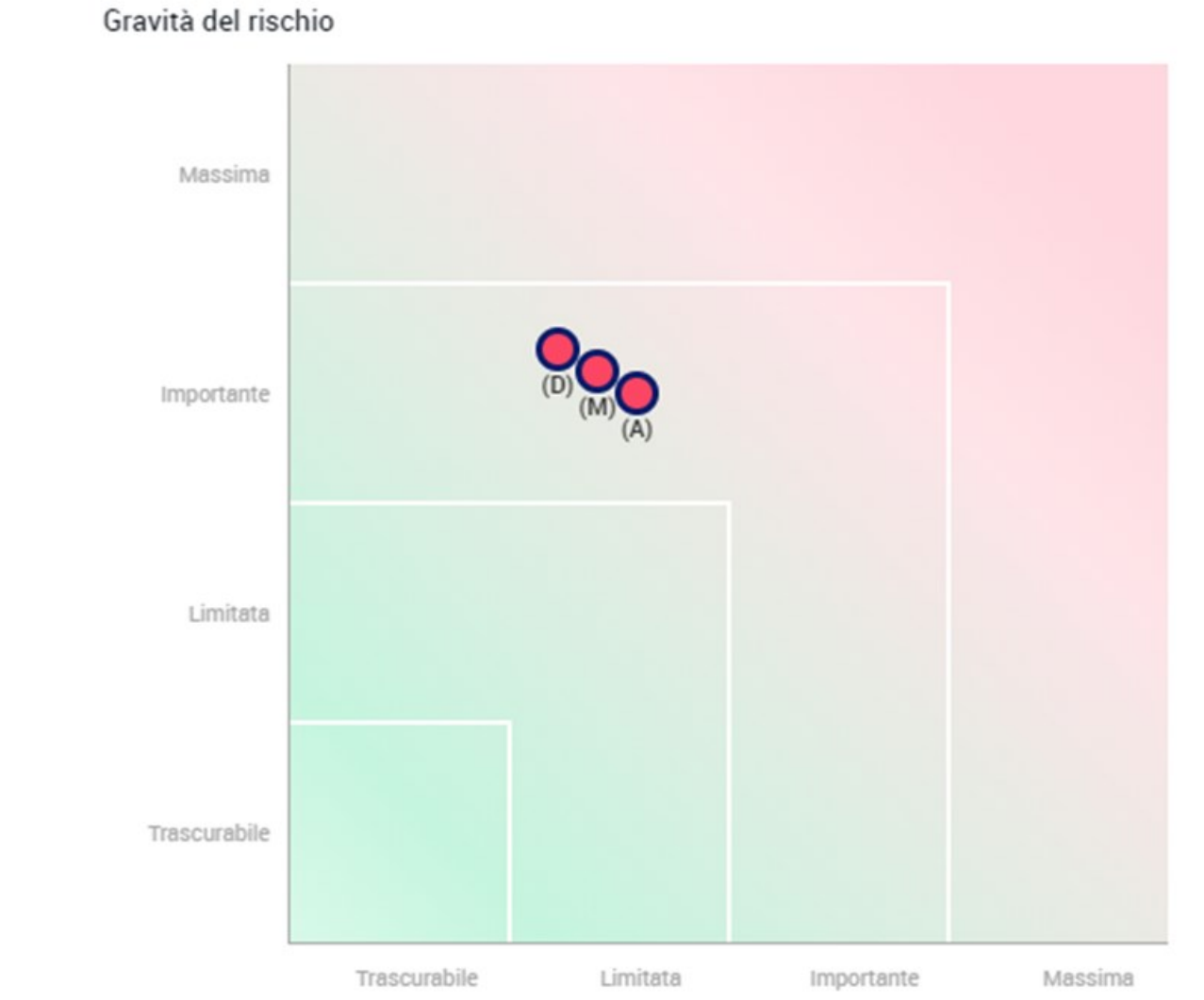
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

Importante.

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

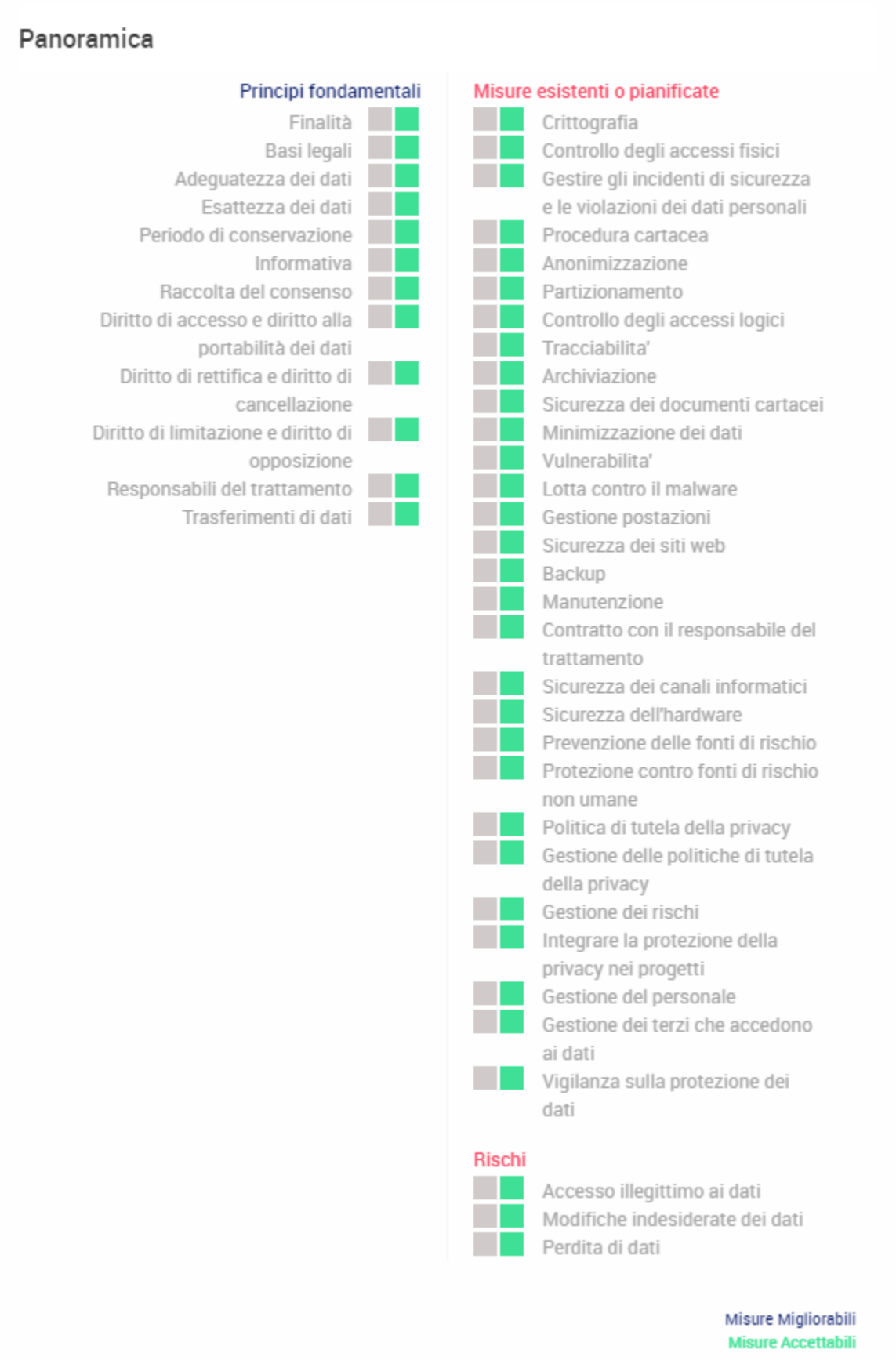
Probabilità del rischio Limitata

Mappatura dei rischi



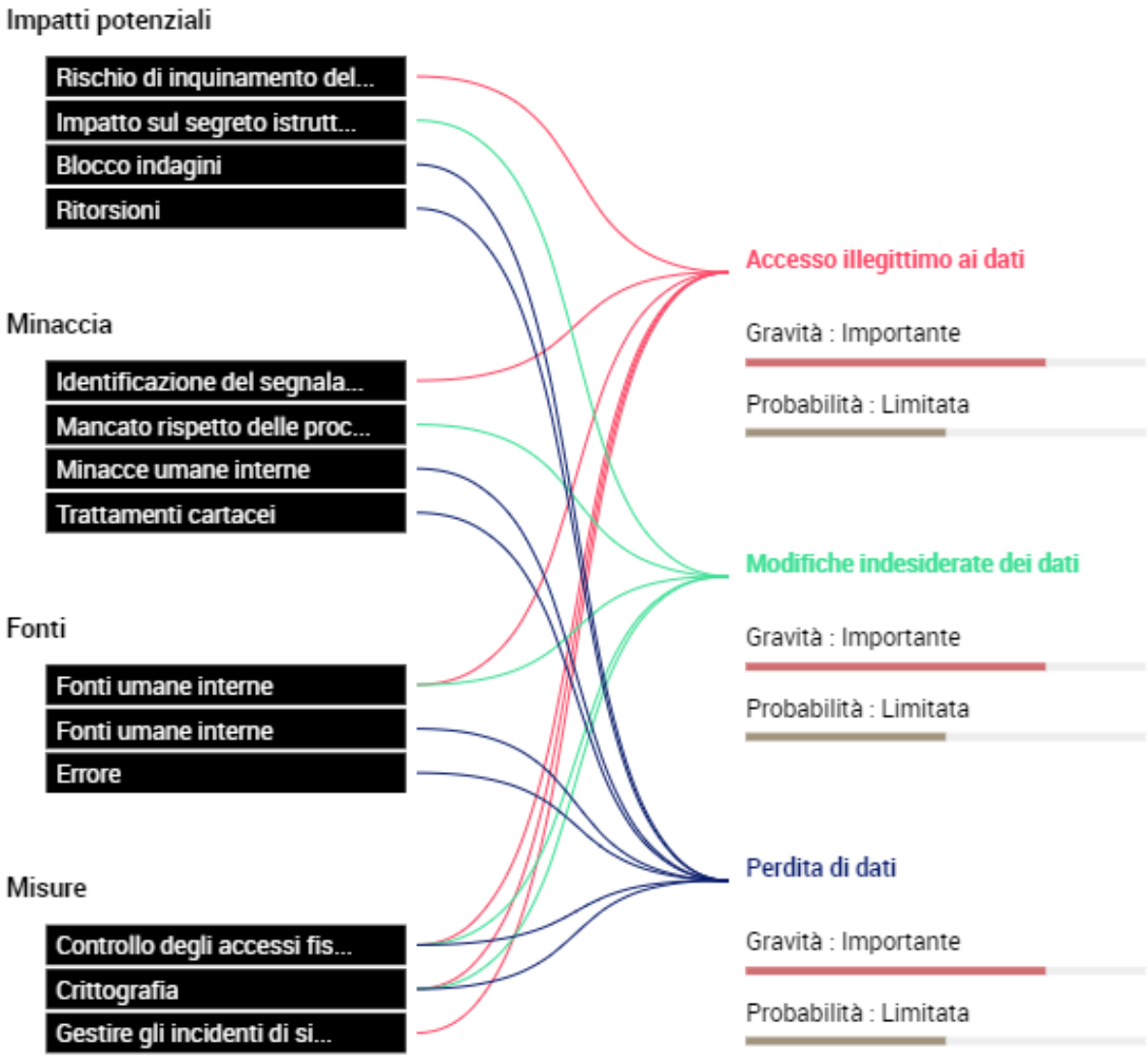
- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Piano d'azione



Rischi

Panoramica dei rischi



Firma DPO

Firma Titolare del trattamento/Delegato