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

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

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

Quali sono le responsabilità connesse al trattamento?

TITOLARE DEL TRATTAMENTO:
Comune

RESPONSABILI DEL TRATTAMENTO:
Whistleblowing Solutions > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing;

Seeweb > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS);

Transaparency International Italia > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing.

Ci sono standard applicabili al trattamento?

Regolamento UE 2016/679 (GDPR);
D.Lgs. 196/03 e s.m.i.;
Direttiva UE 11937/2019;
D. Lgs. 24/2023.

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.

Valutazione : Accettabile

Contesto

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)?

I dati verranno trattati con modalità atte a garantire la riservatezza e la sicurezza delle informazioni, ai sensi degli artt. 25 e 32 del GDPR. Tutte le operazioni in materia, effettuate solo da personale debitamente istruito e autorizzato dai Titolari o loro delegati, avverranno nel rispetto del segreto professionale, del segreto d'ufficio e dei principi di correttezza, liceità e trasparenza, secondo quanto disposto dalla normativa vigente.

Ciclo di vita del trattamento e dei dati:
1) Attivazione della piattaforma;
2) Configurazione della piattaforma;
3) Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti;
4) Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge.

I dati Personali dell'interessato saranno conservati solo per il tempo necessario al perseguimento delle finalità per cui sono stati raccolti e trattati, fatto salvo il maggior tempo necessario per adempiere a obblighi di conservazione cui il Titolare è tenuto in ragione della natura del dato o del documento o per motivi di interesse pubblico o in esecuzione di specifici 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?

Le operazioni di raccolta, registrazione, conservazione e modificazione dei dati personali avverranno attraverso strumenti informatici con logiche strettamente correlate alle finalità indicate nell'informativa resa agli interessati ai sensi dell'art. 13 GDPR.

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?

Il presente trattamento, avente a oggetto i dati personali dell'interessato (qualsiasi informazione relativa alla persona fisica, ivi compreso un numero di identificazione personale), quelli relativi allo stato di salute sarà effettuato esclusivamente per finalità di adempimento agli obblighi di legge.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Regolamento UE 2016/679 (GDPR);
D.Lgs. 196/03 e s.m.i.;
Direttiva UE 11937/2019;
D. Lgs. 24/2023.

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)?

I dati personali raccolti, anche di natura particolare, sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati, nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, in particolare di 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 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.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati personali raccolti, anche di natura particolare, sono esatti e aggiornati, nel rispetto dei principi fissati all'articolo 5 del Regolamento (UE) 2016/679, in particolare di esattezza e aggiornamento dei dati, compresa la tempestiva cancellazione dei dati che risultino inesatti rispetto alle finalità del trattamento.

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?

I dati Personali dell'interessato saranno conservati solo per il tempo necessario al perseguimento delle finalità per cui sono stati raccolti e trattati, fatto salvo il maggior tempo necessario per adempiere a obblighi di conservazione cui il Titolare è tenuto in ragione della natura del dato o del documento o per motivi di interesse pubblico o in esecuzione di specifici obblighi di legg.

Policy di data retention di default delle segnalazioni di 18 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.
Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Valutazione : Accettabile

Principi Fondamentali

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Ai sensi dell'art. 13 del Regolamento UE 2016/679, gli interessati sono informati in merito al trattamento dei loro dati personali, secondo le modalità illustrate nell'informativa istituzionale.

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

La partecipazione alla sperimentazione avviene su base volontaria, libera e consapevole.

Il consenso è ottenuto tramite la sottoscrizione del modulo di consenso al trattamento dei dati .

Il consenso dell'interessato può essere revocato in ogni momento; l'eventuale revoca avrà valore solo per il futuro, restando valido il trattamento eseguito fino a quel momento.

Valutazione : Accettabile

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

La richiesta per l'esercizio dei diritti di accesso e di portabilità dei dati è illustrata nell'informativa sul trattamento dei dati personali, resa agli interessati ai sensi dell'art. 13 del Regolamento UE 2016/679.
La richiesta per l'esercizio dei diritti di accesso e di portabilità dei dati deve essere presentata rivolgendosi direttamente al Titolare.

Valutazione : Accettabile

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

La richiesta per l'esercizio dei diritti di rettifica e cancellazione dei dati è illustrata nell'informativa sul trattamento dei dati personali, resa agli interessati ai sensi dell'art. 13 del Regolamento UE 2016/679.
La richiesta per l'esercizio dei diritti di rettifica e cancellazione dei dati deve essere presentata rivolgendosi direttamente al Titolare.

Valutazione : Accettabile

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

La richiesta per l'esercizio dei diritti di limitazione e di opposizione dei dati è illustrata nell'informativa sul trattamento dei dati personali, resa agli interessati ai sensi dell'art. 13 del Regolamento UE 2016/679.
La richiesta per l'esercizio dei diritti di limitazione e di opposizione dei dati deve essere presentata rivolgendosi direttamente al Titolare.

Valutazione : Accettabile

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

I dati dell'interessato potranno essere trattati con la collaborazione di soggetti "Responsabili del Trattamento" (soggetti esterni che trattano dati per conto del Titolare) e che hanno siglato il relativo accordo a nomina responsabile esterno nel rispetto delle disposizioni dell'art. 28 del GDPR.
L'interessato ha diritto di richiedere l'indicazione del/dei responsabile/i scrivendo ai Titolari del trattamento.

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

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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

Valutazione : Accettabile

Backup

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

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

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.

Valutazione : Accettabile

Rischi

Accesso illegittimo ai dati

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

Impatto trascurabile: dati personali anonimi o pseudonimizzati, dati comuni., Impatto significativo: credenziali amministrative.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Accesso illegittimo ai dati.

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, 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?

Trascurabile,
La gravità del rischio è limitata in quanto le utenze amministrative critiche rappresentano una percentuale minima rispetto al totale dei dati trattati oggetto della valutazione inoltre le misure pianificate sono focalizzate sulla protezione delle utenze critiche.

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

Trascurabile,
Date le misure adottate, focalizzate sulla protezione dei dati critici, la probabilità del rischio è da ritenersi trascurabile.

Valutazione : Accettabile

Rischi

Modifiche indesiderate dei dati

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

Impatto trascurabile: dati personali anonimi o pseudonimizzati, dati comuni., Impatto significativo: credenziali amministrative.

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

Modifiche indesiderate dei dati.

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

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

Crittografia, Controllo degli accessi logici, Tracciabilità, 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, Date le misure adottate, focalizzate sulla protezione dei dati critici, la probabilità del rischio è da ritenersi limitata.

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

Trascurabile,
Date le misure adottate, focalizzate sulla protezione dei dati critici, la probabilità del rischio è da ritenersi trascurabile.

Valutazione : Accettabile

Rischi

Perdita di dati

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

Impatto trascurabile: dati personali anonimi o pseudonimizzati, dati comuni.

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

Perdita di dati.

Quali sono le fonti di rischio?

Fonti umane interne, Fonti umane esterne, Fonti non umane

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

Controllo degli accessi logici, Tracciabilità, 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?

Trascurabile,
La gravità del rischio è trascurabie in quanto le misure pianificate sono focalizzate sulla protezione ed il ripristino dei dati.

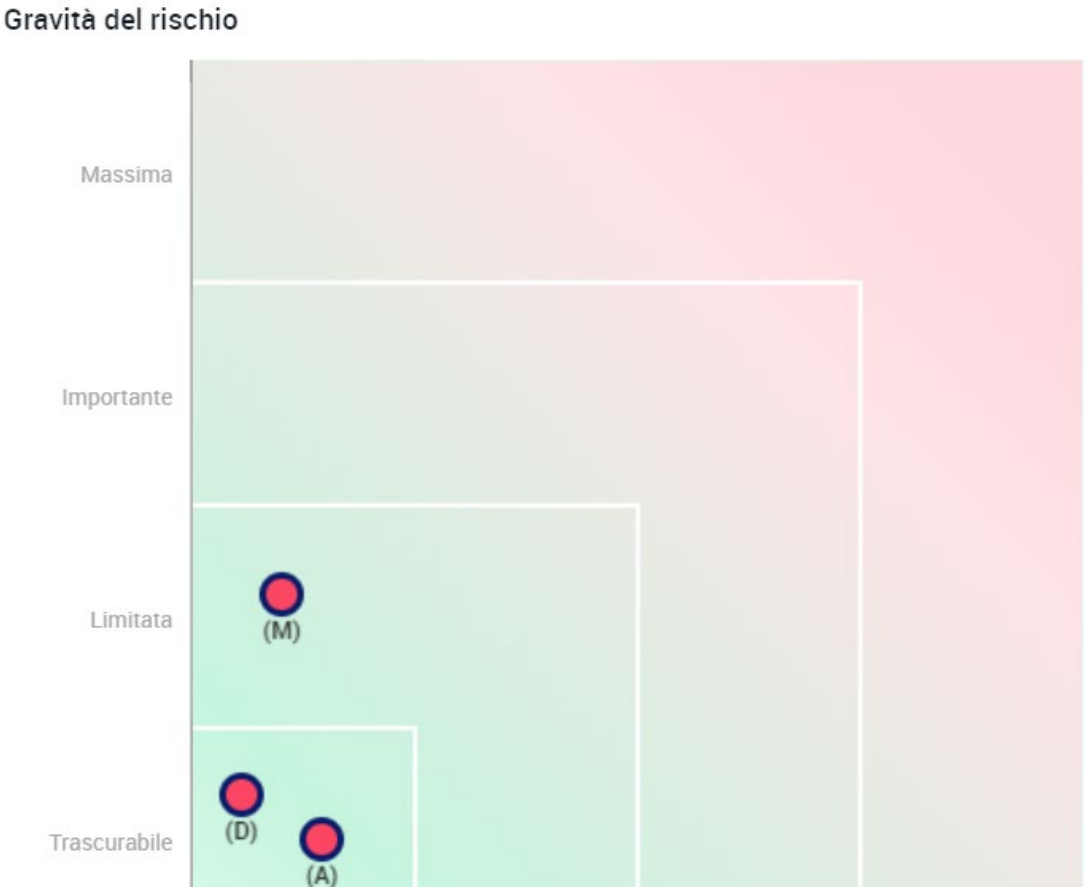
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Trascurabile,
Date le misure adottate, focalizzate sulla protezione dei dati critici, la probabilità del rischio è da ritenersi trascurabile.

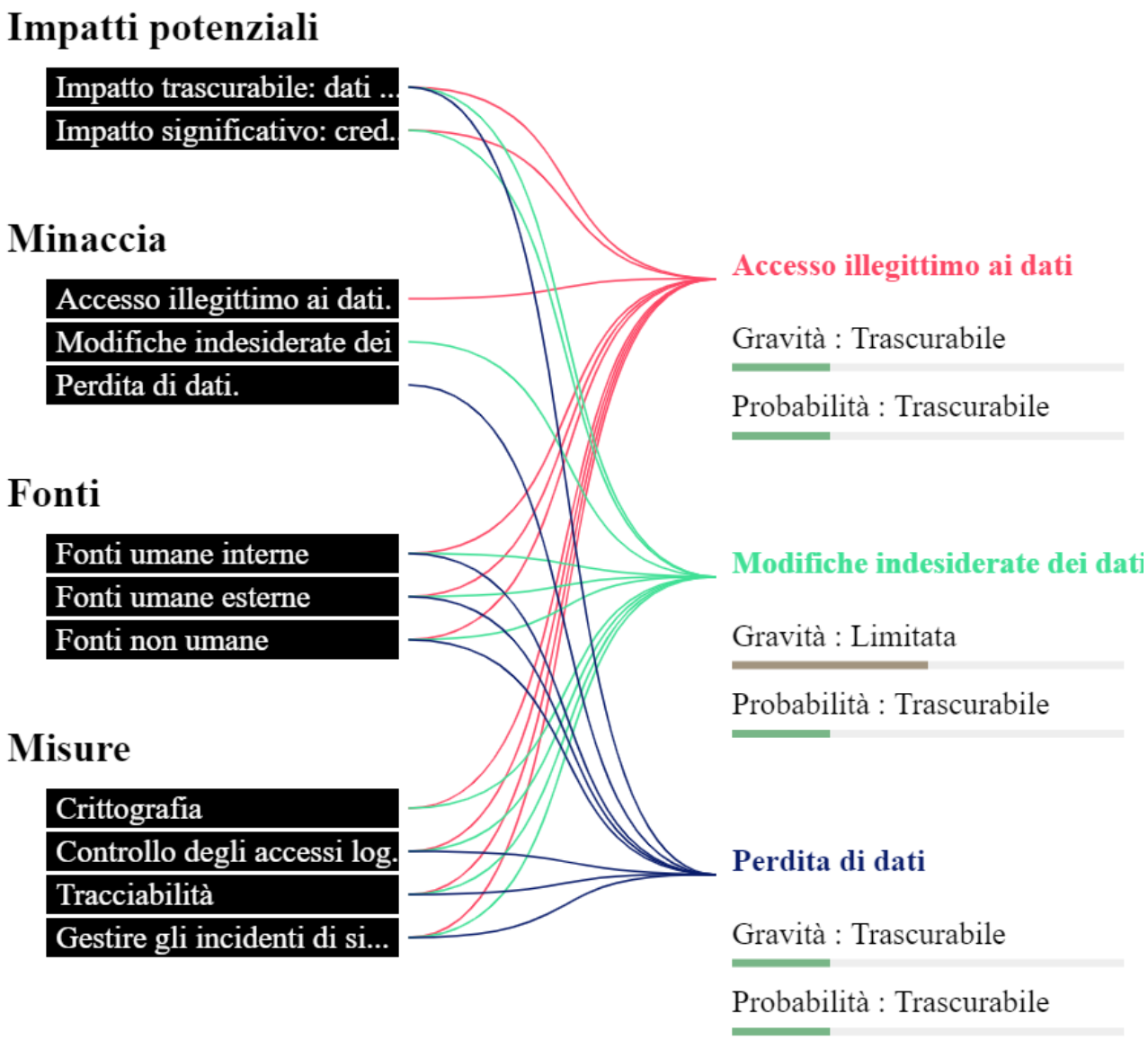
Valutazione : Accettabile

Rischi

Panoramica dei rischi



Mappaggio dei rischi



Piano d'azione

Validazione

DPO and data subjects opinion

Nome del DPO/RPD

DPO

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Il trattamento può essere implementato in quanto rispetta i principi del GDPR.

Richiesta del parere degli interessati

È stato chiesto il parere degli interessati.

Nomi degli interessati

Gli interessati (utenti)

Posizione degli interessati

Il trattamento può essere implementato.

Pareri degli interessati

Il trattamento può essere implementato in quanto rispetta i principi del GDPR.