RIDEMOVI
DPIA
VISSLAN – Piattaforma Whistleblowing

OPINIONE DEL DPO E DEGLI INTERESSATI

Nome del DPO
SZA Studio Legale (Marcello Trabucchi)
Posizione del DPO
Secondo l'opinione del DPO il trattamento può essere implementato.
Richiesta del parere degli interessati
Sono state sentite le organizzazioni sindacali come previsto dal D.lgs. n. 24/2023.

CONTESTO

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento in considerazione è quello effettuato da Ridemovi in seguito alla ricezione e gestione delle segnalazioni di whistleblowing per il tramite della piattaforma messa a disposizione da Visslan.
Quali sono le responsabilità connesse al trattamento?
Il Titolare del trattamento è Ridemovi S.p.A.
Il Responsabile del trattamento è "The Whistle Compliance Solutions AB" proprietaria della piattaforma whistleblowing Visslan.
Ci sono standard applicabili al trattamento?
Visslan si appoggia ai server di AWS per conservare i dati raccolti attraverso la piattaforma.
I server AWS sono situati in Svezia e offrono alti standard di compliance e sicurezza. In particolare, i server AWS vantano le seguenti certificazioni:

- ISO 27001
- ISO 27017
- ISO 27018
- ISO 9001
- CSA STAR CCM v3.0.1

VALUTAZIONE	Accettabile

Dati, processi e risorse di supporto

Quali sono i dati trattati?
I dati trattati riguardano le segnalazioni di whistleblowing ricevute tramite la piattaforma dedicata messa a disposizione di Visslan.
I dati personali oggetto del trattamento sono quelli che il whistleblower decide di comunicare durante la segnalazione. Dunque, il segnalante, se vuole, può lasciare i suoi dati personali come dati anagrafici, informazioni di contatto, può dichiarare se lavora per l'impresa a cui indirizza la segnalazione, può aggiungere i file che ritiene più pertinenti e persino file audio nel caso in cui decidesse di procedere con una segnalazione in forma orale.
Se vuole, il whistleblower può inoltrare anche segnalazioni completamente anonime: il sistema, infatti, non richiede mai di inserire obbligatoriamente dei dati di natura personale (anche semplicemente di contatto).
Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
Il ciclo di vita del trattamento dei dati personali si può sintetizzare nelle seguenti fasi:

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

- 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.

Per effettuare una segnalazione, il whistleblower accede alla piattaforma Visslan dedicata e messa a disposizione da Ridemovi. Nel momento in cui inoltra la segnalazione, il whistleblower riceve un codice univoco della segnalazione che gli dà la possibilità di accedere in qualsiasi momento alla segnalazione effettuata. La segnalazione viene ricevuta dal Case Manager (OdV monocratico) che potrà esaminare la segnalazione e rispondere al whistleblower sempre attraverso la piattaforma. Il Case Manager non conosce l'identità del segnalatore tranne che nel caso in cui quest'ultimo decida di svelarla nella segnalazione o nelle conversazioni successive. Neanche Visslan può vedere le segnalazioni inoltrate dai whistleblower. La piattaforma permette al Case Manager di impostare degli alert per gestire i tempi minimi di risposta. La piattaforma ha preimpostato un termine di conservazione delle segnalazioni allo scadere del quale la segnalazione viene cancellata. Questo termine è modificabile dall'impresa in modo da adattarlo a quanto previsto dalla normativa locale - nel caso di specie 5 anni come previsto dall'art 14 del D.lgs. 24/2023.

Quali sono le risorse di supporto ai dati?

- Full data encryption (256 bit) sia delle segnalazioni whistleblowing e delle comunicazioni con il destinatario
- Supporto HTTPS integrato che sfrutta lo standard TLS 1.3 (SSLabs A+ rating)
- Certificato digitale (Let’s Encrypt)
- Esecuzione di penetration test
- Conformità agli standard e alle best practices in tema di sicurezza delle applicazioni (OWASP)
- Sistema di autenticazione a due fattori (2FA) compliant con lo standard TOTP RFC 6238
- Ambiente sandbox che sfrutta iptables e AppArmor
- Protezione completa contro gli inoltri automatici (prevenzione spam)
- Esecuzione di peer-review e audit di sicurezza periodici
- Supporto PGP per notifiche e-mail criptate
- Non rimangono tracce nelle cache del browser

L'applicazione si sviluppa in due componenti principali: un backend codificato in Python e un Client in JavaScript.

VALUTAZIONE	**Accettabile**

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

La finalità del trattamento consiste nella gestione delle segnalazioni di whistleblowing pervenute alla Società tramite la piattaforma dedicata, in conformità a quanto disposto dal D.lgs. 24/2023 e dal D.lgs. 231/2001.

I dati personali contenuti nelle segnalazioni vengono trattate dall’OdV che effettua le necessarie attività istruttorie volte a verificare la fondatezza della segnalazione. Nel rispetto dei principi di imparzialità e riservatezza, l'OdV effettua ogni attività ritenuta opportuna, inclusa l’audizione del segnalante e di eventuali altri soggetti che possano riferire sui fatti oggetto di segnalazione. Qualora, all’esito delle verifiche, la segnalazione risulti fondata, l'OdV

trasmette l'esito dell'accertamento per approfondimenti istruttori o per l'adozione dei provvedimenti di competenza:

- Al Responsabile HR per l'adozione dei provvedimenti di competenza, ove ne ricorrano i presupposti.
- Se del caso, all'Autorità Giudiziaria o all'Autorità competente ai fini della segnalazione.

VALUTAZIONE	**Accettabile**

Quali sono le basi legali che rendono lecito il trattamento?

Ridemovi effettua il trattamento degli eventuali dati personali contenuti nella segnalazione per adempiere all'obbligo previsto dal D.Lgs 24/2023 nonché per il perseguimento del legittimo interesse a tutelare l'integrità della Società, accertando gli eventuali illeciti segnalati dal whistleblower.

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)?

In piena aderenza con il principio di minimizzazione dei dati, la piattaforma non richiede l'immissione obbligatoria di dati personali, lasciando dunque la libera scelta al whistleblower circa i dati da includere nella segnalazione o nelle successive comunicazioni con il Case Manager. Pertanto, le segnalazioni sono anonime di default e l'indicazione di dati personali propri o di terzi è rimessa alla libera scelta del whistleblower. La piattaforma, inoltre, attraverso una serie di domande volte a circostanziare il fatto segnalato, permette di "guidare" il whistleblower nella procedura di segnalazione limitando la possibilità che vengano inseriti dati non pertinenti.

VALUTAZIONE	**Accettabile**

I dati sono esatti e aggiornati?

I dati sono esatti e aggiornati in quanto vengono direttamente inseriti dal whistleblower.

VALUTAZIONE	**Accettabile**

Qual è il periodo di conservazione dei dati?

Il periodo di conservazione delle segnalazioni è di 5 anni come previsto dall'art. 14 del D.lgs 24/2023.

VALUTAZIONE	**Accettabile**

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Sul sito web della Società è pubblicata l'informativa ex art 13 del GDPR sul trattamento dei dati personali nell'ambito delle segnalazioni whistleblowing.

VALUTAZIONE	**Accettabile**

Ove applicabile: come si ottiene il consenso degli interessati?

Non è applicabile.

VALUTAZIONE	**Accettabile**

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

Come indicato nell'informativa, gli interessati, nei limiti previsti dal GDPR potranno inoltrare una semplice richiesta all'indirizzo dpo@ridemovi.com. Inoltre, il whistleblower potrà controllare in qualunque momento i dati fornito con la segnalazione semplicemente accedendo alla piattaforma whistleblowing utilizzando il codice univoco che identifica la segnalazione.

VALUTAZIONE	**Accettabile**

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

Come indicato nell'informativa, gli interessati, nei limiti previsti dal GDPR potranno inoltrare una semplice richiesta all'indirizzo dpo@ridemovi.com.

VALUTAZIONE	**Accettabile**

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

Come indicato nell'informativa, gli interessati, nei limiti previsti dal GDPR potranno inoltrare una semplice richiesta all'indirizzo dpo@ridemovi.com.

VALUTAZIONE	**Accettabile**

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

La Società "The Whistle Compliance Solutions AB", proprietaria della piattaforma Visslan, è stata designata Responsabile del trattamento con apposito atto che descrive in maniera puntuale gli obblighi e i limiti del trattamento dei dati dalla medesima effettuato in nome e per conto di Ridemovi.

VALUTAZIONE	**Accettabile**

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

I dati vengono trattati all'interno del territorio dell'Unione Europa.

VALUTAZIONE	**Accettabile**

RISCHI

Misure esistenti o pianificate

Sistema di autenticazione

Il sistema utilizza il seguente sistema di autenticazione:

- Il whistleblower può accedere alla propria segnalazione inserendo nella piattaforma il codice univoco (generato randomicamente) di 16 caratteri.
- Credenziali di accesso: quando il Case Manager accede all'interfaccia web della piattaforma deve effettuare il login utilizzando le credenziali di accesso (username e password).

VALUTAZIONE	**Accettabile**

Sicurezza delle password

1. Le password non sono mai conservate in chiaro. Viene utilizzato il servizio Argon2 per fare l'hashing delle password utilizzando una stringa "*salt*" di 128-bit generata randomicamente.

2. Complessità delle password. Il sistema incoraggia l'utilizzo di password forti. Sono definite password "accettabili" quelle formate da almeno 3 input differenti tra: lettere maiuscole, minuscole, numeri e simboli - inoltre, la password deve contenere almeno 10 caratteri e almeno 7 inputs differenti. Sono definite password "forti" quelle formate da lettere maiuscole, minuscole, numeri e simboli, lunghe almeno 12 caratteri e devono contenere almeno 10 inputs differenti.
3. Cambio password obbligatorio. Il sistema obbliga gli utenti a cambiare la password al primo login nonché almeno 1 volta all'anno.

VALUTAZIONE	**Accettabile**

Autenticazione a doppio fattore

Il sistema implementa un sistema di autenticazione a due fattori (2FA) basato su un sistema TOTP (Time-based one-time password) a sua volta basato sull'algoritmo RFC 6238.

VALUTAZIONE	**Accettabile**

Sistema di "Proof of Work" nel Login e Inoltro

Ad ogni login, la piattaforma implementa un sistema automatico di "Proof of Work". Questo sistema obbliga ogni client a risolvere un problema computazionale per poter essere autorizzato a fare il login. La misura è volta a scoraggiare attacchi DoS (denial of service) e altri abusi di servizio come ad es. spam sulla rete.

VALUTAZIONE	**Accettabile**

Controllo dei tentativi di accesso non andati a buon fine

Il sistema individua i tentativi multipli di login non andati a buon fine e attiva una procedura di rallentamento che impone al client di attender 42 secondi prima di completare nuovamente l'autenticazione.

VALUTAZIONE	**Accettabile**

Web Application Security

1. Gestione della sessione: Il sistema assegna a ogni utente autenticato un ID di sessione di 256bits generato randomicamente. Ogni sessione scade dopo 30 minuti o appena l'utente chiude il browser o la scheda su cui è aperta la piattaforma Visslan. L'utente può fare logout anche utilizzando l'apposito bottone previsto dalla piattaforma.
2. Il sistema utilizza un ampio numero di HTTP Headers che sono stati configurati appositamente per migliorare la sicurezza del software e che hanno ottenuto la valutazione A+ sia da Security Headers che dal Mozilla Observatory.
3. Il Backend implementa lo standard CSP (Content Security Policy) e un Permission-policy header che disabilita delle features del browser che potrebbero comportare una de-anonimizzazione degli utenti.

VALUTAZIONE	**Accettabile**

Controllo delle cache

Il sistema usa un HTTP Header che permette il controllo delle cache e, in particolare, impartisce ai browser il comando di non conservare nella cache le informazioni immesse dall'utente.

VALUTAZIONE	**Accettabile**

Anonimizzazione e criptaggio della connessione

Per garantire il completo anonimato degli utenti, il sistema implementa la tecnologia Tor e Onion service v3. La connessione dell'utente, inoltre, è sempre criptata utilizzando il protocollo Tor (quando si utilizza il Browser Tor) oppure il protocollo TLS (quando si utilizza un normale browser).

VALUTAZIONE	**Accettabile**

Application e Network Sandboxing

- **Application:** Il backend di Visslan integra, di default, iptables e utilizza un firewall impostato per permettere connessioni in entrata e in uscita da IP 127.0.0.1 (cd. IP loopback). Inoltre, il sistema applica automaticamente il "network sandboxing" a tutte le comunicazioni in uscita che vengono inviate attraverso Tor.
- **Network:** Il backend di Visslan integra, di default, AppArmour e permette all'applicazione di accedere solo ai file strettamente necessari.

VALUTAZIONE	**Accettabile**

Crittografia dei dati

Tutti i dati, file, messaggi e i metadati scambiati tra il whistleblower e il Case Manager vengono criptati utilizzando il Protocollo di Criptaggio di Visslan, oltre ad ulteriori componenti di criptaggio quali Python-NaCL; PyOpenSSL; Python-Cryptography; Python-GnuPG.

VALUTAZIONE	**Accettabile**

DoS Resiliency

Al fine di evitare DoS alla piattaforma e al database, Visslan cerca di limitare il più possibile l'automatizzazione delle operazioni che richiedono l'interazione umana e monitora attivamente ogni attività volta alla ricerca di attacchi e implementa proattivamente le misure di sicurezza volte a prevenire i DoS.

VALUTAZIONE	**Accettabile**

Cancellazione sicura dei dati

Ogni dato cancellato dall'applicazione viene sovrascritto prima di rendere lo spazio sul disco nuovamente disponibile. La routine di sovrascrittura si articola come segue.
Il file viene sovrascritto una prima volta utilizzando degli 0.
La seconda volta, viene sovrascritto con degli 1.
La terza volta, il file viene sovrascritto con bytes random.

VALUTAZIONE	**Accettabile**

Accesso illegittimo ai dati

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

Soggetti non autorizzati potrebbero venire a conoscenza dei dati contenuti nella segnalazione e potrebbero utilizzarli per fini non inerenti alla segnalazione stessa.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- Utilizzo dei dati per fini diversi da quelli legati alla segnalazione,
- Possibili azioni di ritorsione nei confronti del whistleblower.

Quali sono le fonti di rischio?

- Soggetti esterni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni come ad es. nel caso di attacchi hacker;
- Soggetti interni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

- Sistema di autenticazione;
- Sicurezza delle password;
- Autenticazione a doppio fattore;
- Sistema di "Proof of Work" nel Login e Inoltro;
- Controllo dei tentativi di accesso non andati a buon fine;
- Web Application Security;
- Controllo delle cache;
- Anonimizzazione e criptaggio della connessione;
- Application e Network Sandboxing;
- Crittografia dei dati;
- DoS Resiliency;
- Cancellazione sicura dei dati.

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

Trascurabile. La piattaforma non richiede all'utente di inserire dati che possano identificarlo - anzi, permette delle segnalazioni completamente anonime. Dunque, le informazioni inserite dal whistleblower non sempre contengono dati personali (propri o di terzi).

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

Trascurabile. Le misure di sicurezza adottate dal fornitore della piattaforma sono in linea con gli standard applicati nel settore per la limitazione del rischio di accesso illegittimo ai dati.

VALUTAZIONE	**Accettabile**

Modifiche indesiderate dei dati

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

- Gestione errata della segnalazione;
- Modifica dei dati che potrebbe produrre una segnalazione che non rispecchia il problema segnalato;
- Attribuzione di un comportamento scorretto a un soggetto diverso da quello originariamente segnalato o attribuzione al soggetto segnalato di un comportamento scorretto differente da quello segnalato;
- Il segnalato potrebbe essere oggetto di investigazioni ulteriori o non dovute.

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

- Possibili azioni di sabotaggio;
- Accessi non autorizzati ai dati.

Quali sono le fonti di rischio?

- Soggetti esterni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni come ad es. nel caso di attacchi hacker;

- Soggetti interni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni.

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

- Sistema di autenticazione;
- Sicurezza delle password;
- Autenticazione a doppio fattore;
- Sistema di "Proof of Work" nel Login e Inoltro;
- Controllo dei tentativi di accesso non andati a buon fine;
- Web Application Security;
- Controllo delle cache;
- Anonimizzazione e criptaggio della connessione;
- Application e Network Sandboxing;
- Crittografia dei dati;
- DoS Resiliency;
- Cancellazione sicura dei dati.

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

Trascurabile. Le segnalazioni sono sempre seguite da un'attività investigativa volta ad accertarne la fondatezza. Dunque, anche in caso di modifica indesiderata dei dati della segnalazione, l'organizzazione pone in essere una procedura aziendale che permetterebbe di evitare l'adozione di provvedimenti nei confronti di un soggetto che non ha alcuna responsabilità.

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

Trascurabile. Le misure di sicurezza adottate dal fornitore della piattaforma sono in linea con gli standard applicati nel settore per la limitazione del rischio di modifiche indesiderate dei dati.

VALUTAZIONE	**Accettabile**

Perdita di dati

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

Impossibilità di dar seguito alle segnalazioni whistleblowing.

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

- Data breach;
- Comportamento fraudolento da parte dei soggetti deputati alla gestione della segnalazione;
- Azione di sabotaggio informatico.

Quali sono le fonti di rischio?

- Soggetti esterni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni come ad es. nel caso di attacchi hacker;
- Soggetti interni all'organizzazione che accedono ai dati senza avere le necessarie autorizzazioni.

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

- Sistema di autenticazione;

- Sicurezza delle password;
- Autenticazione a doppio fattore;
- Sistema di "Proof of Work" nel Login e Inoltro;
- Controllo dei tentativi di accesso non andati a buon fine;
- Web Application Security;
- Controllo delle cache;
- Anonimizzazione e criptaggio della connessione;
- Application e Network Sandboxing;
- Crittografia dei dati;
- DoS Resiliency;
- Cancellazione sicura dei dati.

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

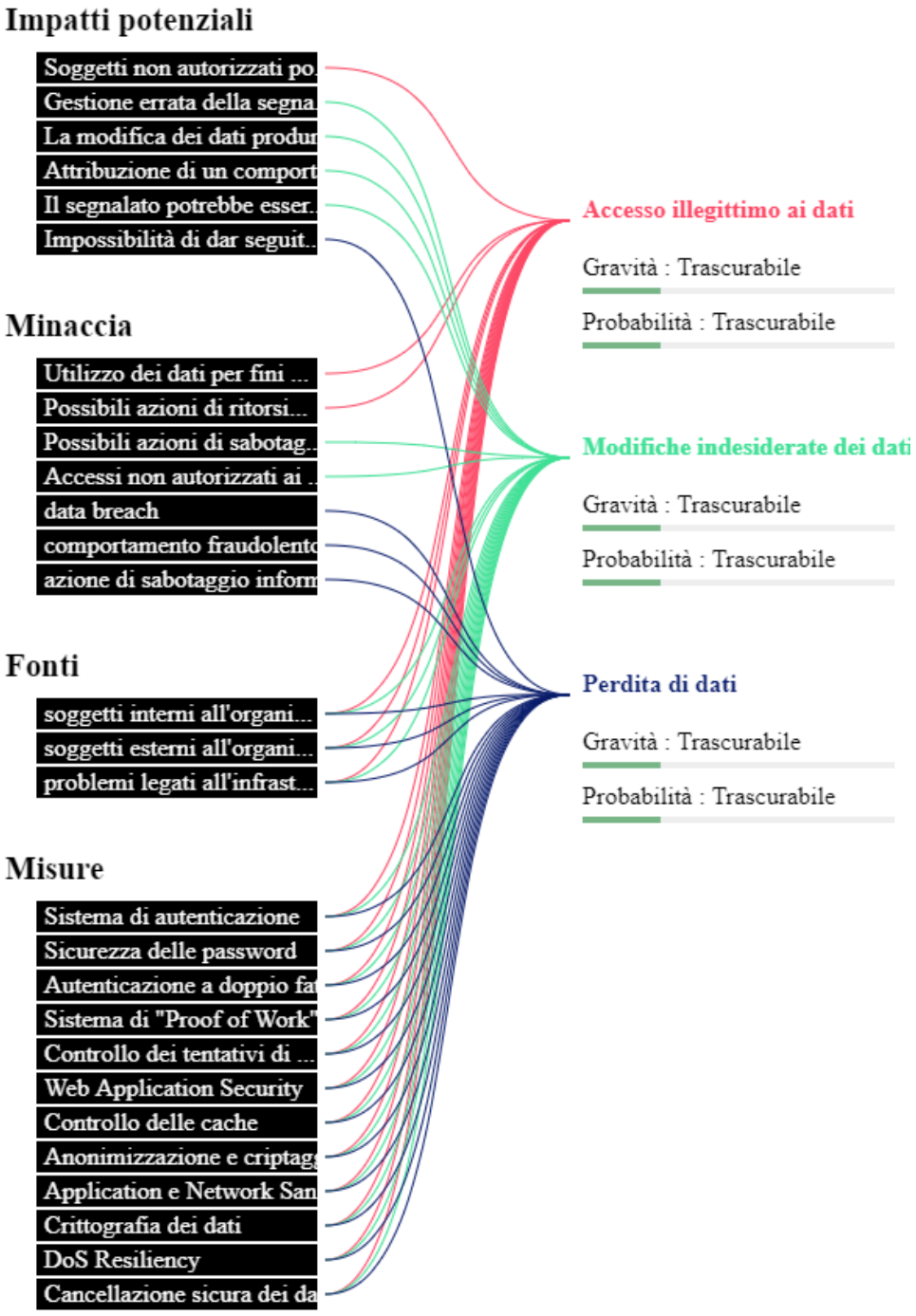
Trascurabile. La probabilità che il rischio si materializzi è mitigata da tutte le misure di sicurezza adottate dall'organizzazione e in particolare dalle misure di carattere informatico che proteggono le infrastrutture dove tali dati vengono conservati e trattati.

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

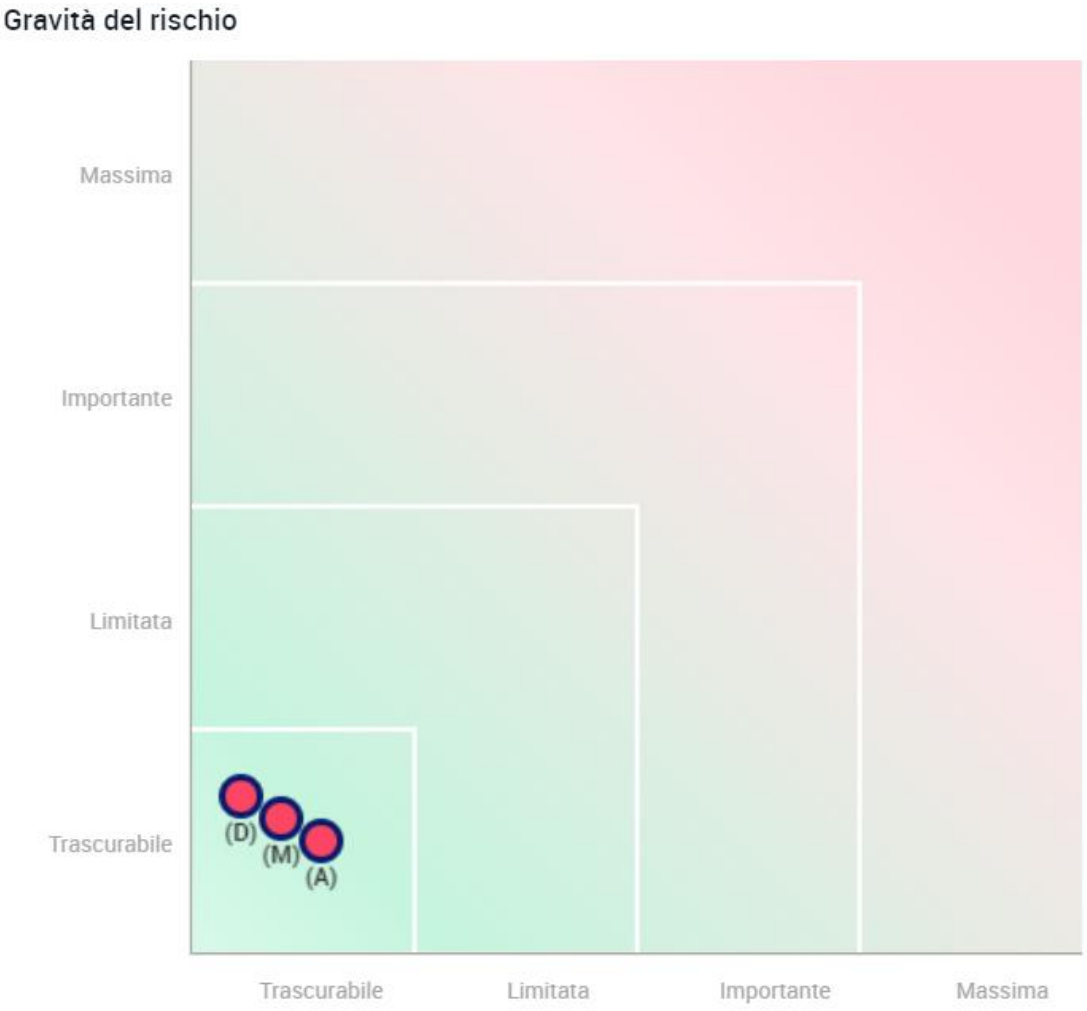
Trascurabile. Le misure di sicurezza adottate dal fornitore della piattaforma sono in linea con gli standard applicati nel settore per la limitazione del rischio di perdita dei dati.

VALUTAZIONE	**Accettabile**

Panoramica dei rischi


Impatti potenziali
Soggetti non autorizzati po
Gestione errata della segna
La modifica dei dati produ
Attribuzione di un comport
Il segnalato potrebbe esser
Impossibilità di dar seguit
Minaccia
Utilizzo dei dati per fini ...
Possibili azioni di ritorsi...
Possibili azioni di sabotag
Accessi non autorizzati ai
data breach
comportamento fraudolento
azione di sabotaggio inform
Fonti
soggetti interni all'organi...
soggetti esterni all'organi...
problemi legati all'infrast...
Misure
Sistema di autenticazione
Sicurezza delle password
Autenticazione a doppio fa
Sistema di "Proof of Work"
Controllo dei tentativi di ...
Web Application Security
Controllo delle cache
Anonimizzazione e criptag
Application e Network San
Crittografia dei dati
DoS Resiliency
Cancellazione sicura dei da
Accesso illegittimo ai dati
Gravità : Trascurabile
Probabilità : Trascurabile
Modifiche indesiderate dei dati
Gravità : Trascurabile
Probabilità : Trascurabile
Perdita di dati
Gravità : Trascurabile
Probabilità : Trascurabile

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

Panoramica