VALUTAZIONE DI IMPATTO PRIVACY DEL SERVIZIO DI WHISTLEBLOWING

AUTORE: RABINO Roberta

REVISORE: Davide Bertone

VALUTATORE: DPO Chiara Vaccari

La presente *Data Protection Impact Assessment* (in seguito DPIA), condotta ai sensi dell'art. 35 GDPR, ha lo scopo di descrivere il trattamento di dati personali connesso al servizio fornito dalla società Whistleblowing Solutions, valutarne la necessità e la proporzionalità e determinare l'origine, la natura, la particolarità e la gravità degli eventuali rischi per i diritti e le libertà delle persone fisiche. L'esito di tale valutazione dovrebbe essere considerato nella definizione delle ulteriori misure da adottare per dimostrare che il trattamento dei dati personali rispetta il Regolamento (UE) 2016/679 (in seguito GDPR).

Contesto – panoramica del trattamento

Quale è il trattamento in considerazione?

Utilizzo di piattaforma in esternalizzazione per il servizio di Whistleblowing

Quali sono le responsabilità connesse al trattamento?

Titolare del Trattamento: Comune di Busca
Responsabile del Trattamento: Whistleblowing Solutions
Sub-responsabili: Seeweb e Transparency International Italia

Ci sono standard applicabili al trattamento?

Misure adeguate di sicurezza del trattamento dei dati personali

VALUTAZIONE: ACCETTABILE

Contesto – Dati, processi e risorse di supporto

Quali sono i dati trattati?

Dati necessari per la registrazione dell'utente:
Nome, cognome, ruolo, email, telefono
Dati contenuti nella segnalazione riguardanti il segnalante o altri soggetti, anche eventualmente dati particolari o dati relativi a condanne penali o reati, qualora contenuti nella segnalazione

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

Il trattamento avviene, una volta installata la piattaforma, con l'inserimento e la segnalazione da parte dell'interessato, quindi il successivo accesso da parte dell'incaricato alla lavorazione e, a processo terminato, la cancellazione al termine del periodo di conservazione individuato

Quali sono le risorse di supporto ai dati?

Architettura di sistema composta da:
- un cluster di due firewall perimetrali
- un cluster di due firewall fisici dedicati
- una Storage Area Network pienamente ridondata.

Il software Global Leaks, open source, di cui Whistleblowing Solutions è co-sviluppatore.
Altri software per source per la virtualizzazione quale WmWare, firewall, sistema operativo, VPN.

VALUTAZIONE: ACCETTABILE

Principi fondamentali – proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento è necessario per consentire agli utenti di segnalare gli illeciti ai sensi del D.Lgs 24/2023

Quali sono le basi legali che rendono lecito il trattamento?

Il trattamento è necessario per l'adempimento di un contratto tra le parti e per l'adempimento di un obbligo di legge

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 trattati sono quelli strettamente necessari al funzionamento della piattaforma (nome, cognome, mail telefono, ruolo)

I dati sono esatti e aggiornati?

Esattezza e aggiornamento dei dati sono a cura dell'utente che utilizza la piattaforma

Qual è il periodo di conservazione dei dati?

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 dalla piattaforma 15 giorni dopo la disattivazione del servizio.

VALUTAZIONE: ACCETTABILE

Principi fondamentali – misure a tutela degli interessati

Come sono informati del trattamento gli interessati?

Il trattamento è effettuato in conformità alle disposizioni di legge e gli interessati sono informati ai sensi dell'art. 13 GDPR

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non è richiesto per la tipologia di trattamenti

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

Gli interessati possono esercitare i proprio diritti contattando il Titolare ai recapiti indicati nell'informativa ex. Art. 13 GDPR

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

Gli interessati possono esercitare i proprio diritti contattando il Titolare ai recapiti indicati nell'informativa ex. Art. 13 GDPR

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

Gli interessati possono esercitare i proprio diritti contattando il Titolare ai recapiti indicati nell'informativa ex. Art. 13 GDPR

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

Si, sono definiti i ruoli di responsabili e sub-responsabili tramite apposite nomine

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

I dati sono trattati esclusivamente in Italia e comunque nel territorio dell'Unione Europea-
Non vi è alcun trasferimento di dati al di fuori dell'Unione Europea.

VALUTAZIONE: ACCETTABILE

Rischi – misure esistenti o pianificate

Crittografia

L'applicativo GlobalLeaks implementa uno specifico protocollo crittografico. Ogni informazione viene protetta da protocollo TLS 1.2+ con SSLLabs rating a+.

Controllo degli accessi logici

L'accesso all'applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.
Il sistema implementa policy password sicura e vieta il riutilizzo

Tracciabilità

L'applicativo GlobalLeaks 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 GlobalLeaks implementa un database SQLite con elevate garanzie di sicurezza

Gestione delle vulnerabilità tecniche

Periodici audit di sicurezza indipendenti sugli applicativi, su base almeno annuale. Tutti i report vengono pubblicati.
Si aggiunge una peer review indipendente realizzata dagli stake holder

Backup
Backup remoto giornaliero con policy retention di 7 giorni necessaria per finalità di disaster recovery

Manutenzione
Manutenzione periodica

Sicurezza dei canali informatici
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
Datacenter provenienti da un'infrastruttura con controllo degli accessi, monitoraggio 24/7 con videosorveglianza, sistema di allarme e barriere fisiche.
Datacenter certificati ISO 27001.

Gestione degli incidenti di sicurezza e violazioni dei dati
Whistleblowing Solutions ha definito una procedura di gestione dei data breach

Lotta al malware
Tutti i computer sono dotati di antivirus e firewall e il personale riceve formazione adeguata.

VALUTAZIONE: ACCETTABILE

Rischi – Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Esposizione dei dati degli utenti, esposizione del contenuto della segnalazione dell'utente, esposizione dei dati dell'ente

Quali sono le principali minacce che potrebbero concretizzare il rischio
Sottrazione di dati tramite accesso abusivo al sistema

Quali sono le fonti di rischio?
Attacchi informatici, utilizzo improprio da parte del personale

Quali misure tra quelle individuate contribuiscono a mitigare il rischio?
Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dell'hardware, Lotta al malware

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la gravità del rischio

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

Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la probabilità del rischio

VALUTAZIONE: ACCETTABILE

Rischi – modifiche indesiderate dei dati

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

Modifiche del contenuto delle segnalazioni, modifiche dei dati degli utenti segnalatori, modifiche dei dati dell'ente.

Quali sono le principali minacce che potrebbero concretizzare il rischio

Accesso e modifica di dati tramite accesso abusivo al sistema

Quali sono le fonti di rischio?

Attacchi informatici, utilizzo improprio da parte del personale

Quali misure tra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dell'hardware, Lotta al malware

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

Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la gravità del rischio

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

Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la probabilità del rischio

VALUTAZIONE: ACCETTABILE

Rischi – Perdita di dati

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

Perdita di dati relativi alla segnalazione, degli utenti e dell'ente.

Quali sono le principali minacce che potrebbero concretizzare il rischio

Perdita di dati tramite accesso abusivo al sistema

Quali sono le fonti di rischio?

Attacchi informatici, utilizzo improprio da parte del personale

Quali misure tra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dell'hardware, Lotta al malware

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

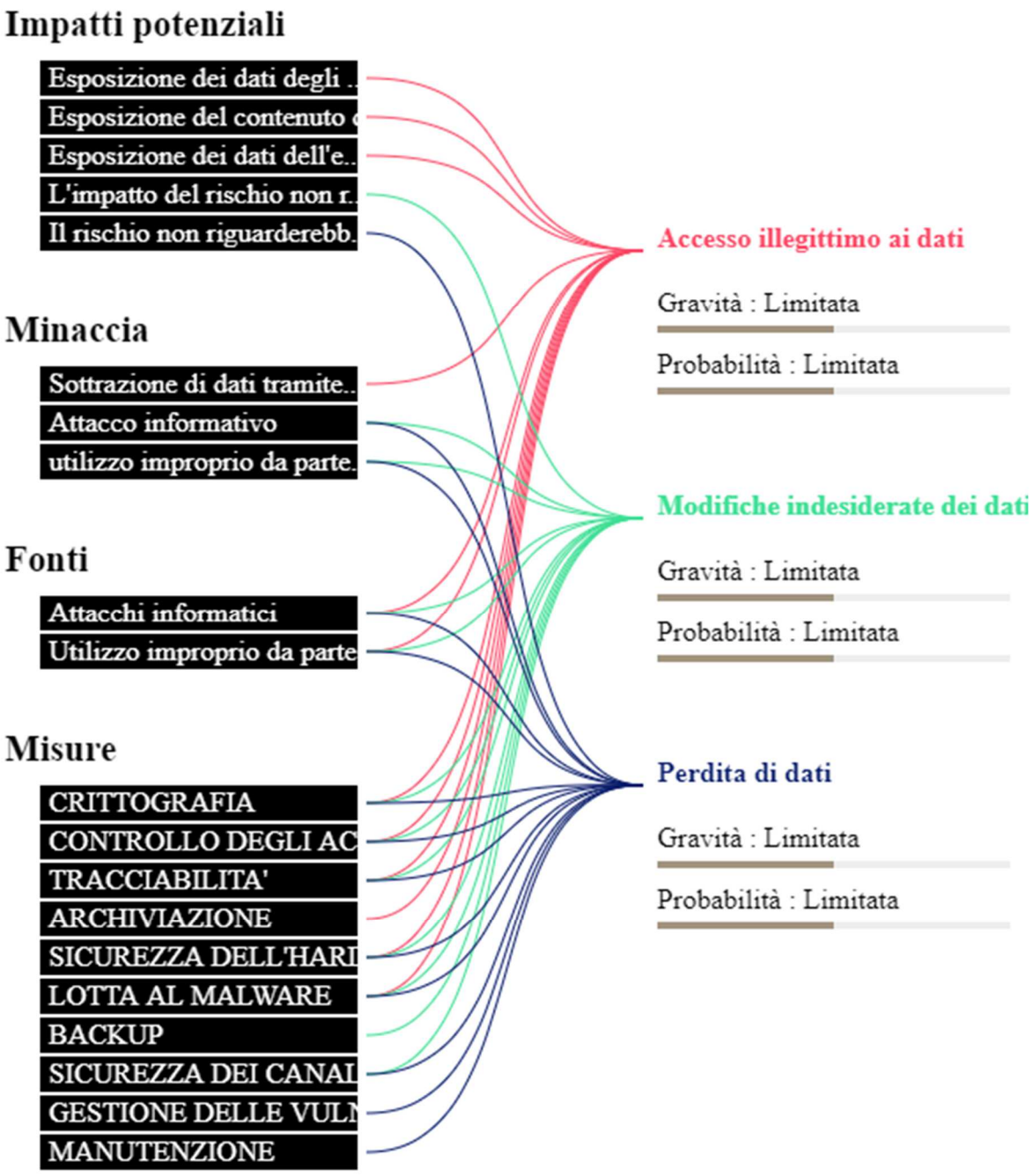
Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la gravità del rischio

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

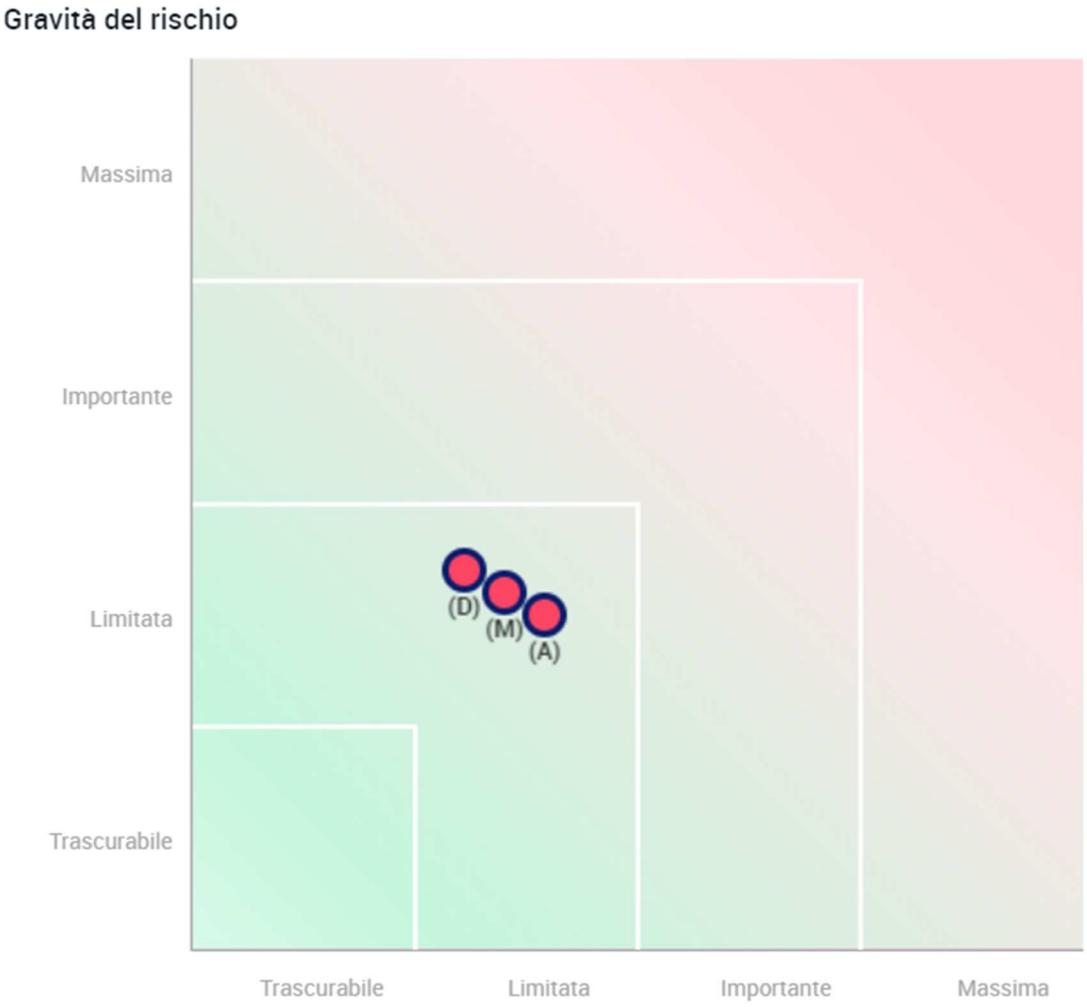
Limitata, le misure tecniche ed organizzative adottate contribuiscono a ridurre la probabilità del rischio

VALUTAZIONE: ACCETTABILE

Rischi – Panoramica dei rischi

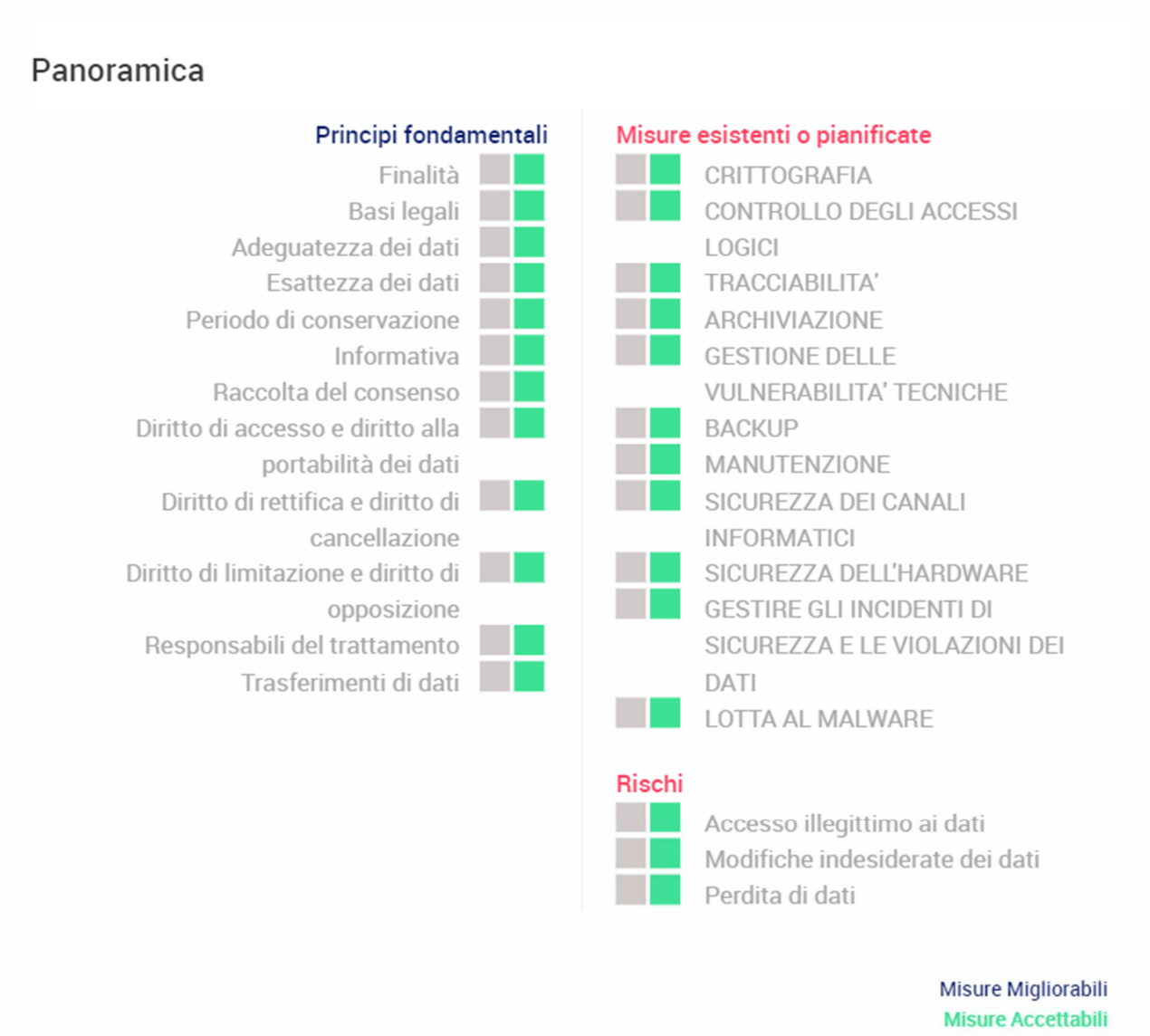


Rischi – Mappaggio dei rischi



- 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



Parere del DPO

Nome del DPO

Chiara Vaccari

Posizione del DPO

Il trattamento può essere implementato

Parere del DPO

Il DPO ritiene che sussistano adeguate misure tecniche ed organizzative che limitano il rischio

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati

Motivazione della mancata richiesta del parere degli interessati

Tenuto conto della portata europea della norma e della platea di interessati, la richiesta di parere risulterebbe eccessivamente onerosa. Si sottolinea inoltre che Whistleblowing Solutions è una impresa sociale che esercita un'attività di interesse generale, senza scopo di lucro e per finalità civiche, solidaristiche e di utilità sociale.