Data Privacy Impact Assessment (DPIA)

Whistleblowing – Piattaforma Web

Unione Montana dei Comuni del Mugello

1. Premessa

Ai sensi dell'art. 35 del Regolamento UE n. 2016/679 (in seguito "GDPR"), ogni qualvolta si debba iniziare un trattamento che possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, è necessario predisporre una DPIA, in particolare se il trattamento è connesso all'impiego di nuove tecnologie.

La DPIA (Data Protection Impact Assessment) corrisponde alla valutazione d'impatto del trattamento dei dati personali. Si dovranno considerare la natura, il contesto e le finalità del trattamento ed i rischi collegati.

La DPIA consente al Titolare del trattamento di prendere visione del rischio prima di procedere al trattamento in modo da annullare o quantomeno ridurre fortemente i rischi connessi al trattamento.

Il rischio residuo dovrà essere valutato in funzione della finalità e del diritto/dovere in capo al Titolare di eseguire tale trattamento.

I principi fondamentali della DPIA risultano pertanto:
- i diritti e le libertà fondamentali dell'interessato, punto fondante dell'intero impianto del GDPR;
- i trattamenti dei dati personali attraverso l'analisi della tipologia dei dati, gli strumenti che si intende utilizzare, le procedure e l'organizzazione del lavoro.
- la gestione dei rischi per la privacy, attraverso le misure tecniche ed organizzative di volta in volta adeguate rispetto al rischio sia digitale che analogico (sicurezza fisica del dato elettronico, del dato cartaceo e di ogni contenitore dei dati elettronici e cartacei).

2. Contesto

2.1. Panoramica del trattamento

Il trattamento ha ad oggetto i dati personali dei soggetti che effettuano segnalazioni e dei soggetti segnalati ai sensi del D.lgs. n. 24/2023.

La gestione delle segnalazioni effettuata attraverso piattaforma web (canale interno) sarà affidata a Responsabile esterno individuato in Whistleblowing Solutions (di seguito indicato anche "Fornitore").

Sarà utilizzata piattaforma esterna ma il Fornitore dovrà soltanto "conservare" i dati crittografati (quindi ad esso non accessibili) e garantire misure adeguate.

2.2 Architettura di Sistema

Di seguito riportiamo le caratteristiche tecniche comunicate dal Fornitore all'interno del documento "DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI".

Il sistema è composto da:

- Un cluster di due firewall perimetrali;

- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

Il software impiegato è basato su codice open-source GlobaLeaks di cui il fornitore è co-autore e coordinatore di progetto.

Le tecnologie impiegate sono:

- Debian/Linux (S.O. utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (VPN);
- VMware (software di virtualizzazione)
- Veeam (software di backup)
- Plesk (software per realizzazione siti web)

Predisposizione dei sistemi virtualizzati:

- I server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
- Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);
- Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
- Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

2.3 Architettura di Rete

- L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente;
- Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definito insieme di amministratori di sistema;
- Ogni connessione di rete implementa TLS 1.2̆;
- Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents;
- L'applicativo GlobaLeaks abilita 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.

2.4 Collegamento a piattaforma Web

Per tutelare la riservatezza del segnalante:

- Tutti i dispositivi utilizzati non registrano alcuna informazione in file di log (es. ip address, user agents);
- L'applicativo può essere utilizzato anche da browser Tor (per aumentare la sicurezza di anonimato).

2.5 Responsabilità connesse al trattamento

Ruolo	Nominativo
Titolare del trattamento	UNIONE MONTANA DEI COMUNI DEL MUGELLO
Delegato al trattamento	Responsabile della prevenzione della corruzione e della trasparenza (RPCT)

2.6 Standard applicabili al trattamento

Al trattamento in materia di segnalazioni e normativa whistleblowing si applicano le seguenti normative e standard.

Regolamento UE n. 2016/679 (c.d. GDPR)

D.lgs. n. 196/2003 (c.d. Codice Privacy) così come modificato dal D.lgs. n. 101/2018

Direttiva UE 1937/2019

D.lgs. n. 24/2023

2.7 Dati personali e Interessati

Di seguito si riportano le tipologie di dati personali che sono oggetto di trattamento a seguito di una segnalazione fatta ai sensi del D.lgs. n. 24/2023

Categoria di dato personale Categoria di interessato

I dati personali potranno riguardare Dipendenti, Collaboratori e Fornitori che effettuano una segnalazione o che ne sono oggetto.

Dati personali comuni (es. dati di contatto).

Dati personali particolari (es. dati relativi alla salute, condanne penali)

2.8 Rischi per gli interessati

La mancata protezione dei dati personali delle persone coinvolte nella segnalazione (segnalante, segnalato, facilitatore ed altre persone previste per legame parentale o affettivo al segnalante) può comportare conseguenze personali come ritorsioni, giudizi sommari, discriminazioni.

3. Principi Fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi

Il trattamento è finalizzato esclusivamente alla gestione della segnalazione e all'adempimento degli obblighi legali previsti dalla normativa vigente in materia di whistleblowing.

Il trattamento si fonda sulla base giuridica dell'adempimento di un obbligo di legge a cui è tenuto il titolare (GDPR 679/2016 art. 6.1. lett. c). Riguardo a talune comunicazioni riguardanti il segnalante, potrebbe essere necessario il consenso per procedere a specifici trattamenti.

I dati personali raccolti sono solo quelli espressamente necessari alla gestione della segnalazione, come normativamente previsto dall'articolo 12 del D.lgs. n. 24/2023. Il perseguimento delle finalità avviene nel rispetto del principio di minimizzazione (GDPR 679/2016 art. 5.1. lett. c).

I dati personali relativi alla segnalazione possono essere comuni e particolari e vengono ritenuti indispensabili dal segnalante in fase di segnalazione o dalla persona incaricata dal Titolare in fase di verifica della segnalazione.

I dati personali relativi alle segnalazioni sono costantemente aggiornati e integrati da parte della persona incaricata della gestione delle segnalazioni e possono essere aggiornati e integrati dal segnalante.

Le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e per ulteriore periodo necessario a poter provare di aver adempiuto agli obblighi di legge.

Il trattamento è sempre preceduto da informativa come meglio indicato al punto 3.1.

Il periodo di conservazione non potrà essere superiore a cinque anni.

3.1. Misure a tutela dei diritti degli interessati

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR 679/2016.

L'informativa viene resa disponibile secondo le seguenti modalità:

- Affissione negli uffici

- Pubblicazione sito internet – sezione dedicata al Whistleblowing

Il trattamento dei dati personali relativi la segnalazione da parte dei soggetti espressamente autorizzati al trattamento non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge (Art. 6.1. lett. c) del GDPR).

Nel caso invece ricorra l'ipotesi di comunicazione dei dati personali a soggetti diversi da quelli espressamente autorizzati dal Titolare, il segnalante dovrà prestare il proprio consenso.

Gli interessati possono esercitare i diritti previsti dagli artt. 15 ss. del GDPR 679/2016 attraverso i canali di comunicazione indicati nell'informativa.

Le terze parti che trattano dati personali per conto del Titolare sono state nominate Responsabili del trattamento ai sensi dell'art. 28 GDPR, attraverso contratti specifici.

Per questa tipologia di trattamento non è previsto un trasferimento di dati personali fuori dall'Unione Europea.

4. Misure esistenti

Per quanto riguarda il canale di segnalazione web (whistleblowing.it), i dati saranno trasmessi in modalità protetta in transito da protocollo TLS 1.2+ con SSLLabs rating A+.

Nessun dato sarà salvato "in chiaro" sui supporti di memorizzazione utilizzati dal Responsabile del trattamento.

Ogni informazione sarà protetta con chiave asimmetrica personale.

Il sistema è installato su S.O. Linux su cui è attiva Full Disk Enscryption (FDE).

Questa scelta garantisce la riservatezza del dato anche in caso di accesso non autorizzato agli strumenti di memorizzazione e di backup.

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 di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema di 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 sistemi di backup sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

I datacenter del fornitore dispongono di infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza a circuito chiuso oltre a sistema di allarme e barriere fisiche presidiate 7x24.

I datacenter del fornitore sono certificati ISO 27001.

5. Rischi

I rischi per i dati personali sono

- Accesso non autorizzato / Perdita di riservatezza
- Perdita dei dati

5.1 Accesso non autorizzato

Un accesso non autorizzato può avvenire per

- Attività di hacking
- Penetrazione nei locali dove sono conservati gli strumenti di memorizzazione
- Sottrazione di credenziali

5.1.1 Attività di hacking

La struttura informatica e sistemistica del Fornitore rende improbabile tale rischio (firewall, collegamento vpn, crittografia nella comunicazione).

5.1.2 Accesso non autorizzato ai locali

Il sistema di sicurezza del fornitore (videosorveglianza a circuito chiuso, vigilanza 7x24) rende improbabile tale rischio.

5.1.3 Sottrazione delle credenziali

Il Titolare del trattamento autorizzerà soltanto una persona ad accedere alla piattaforma web.

Come indicato dalla normativa, la persona designata sarà il responsabile della prevenzione della corruzione e della trasparenza (RPCT).

Questa figura è formata riguardo la riservatezza e la protezione dei dati personali e quindi delle componenti riservate per l'accesso ai dati stessi.

Considerando la preparazione e l'affidabilità dimostrata dalla persona che sarà designata, si ritiene poco probabile tale evento.

Saranno comunicate tutte le informazioni necessarie ad una corretta gestione dei dati di accesso alla piattaforma e dei dati personali ivi contenuti oltre alle procedure successive da seguire per espletare il compito assegnato.

5.2 Perdita di dati
La perdita di dati può avvenire per

- Guasto hardware
- Attività di hacking
- Evento esterno (terremoto, incendio, accesso non autorizzato)

In ogni caso, le copie di backup delocalizzate aumentano notevolmente la sicurezza di disponibilità dei dati in caso di perdita che rimane comunque un rischio marginale.

5.2.1 Guasto hardware
Il Fornitore utilizza macchine virtuali e server dedicati ridondanti oltre a backup che mantiene per 7 giorni.

5.2.2 Attività di hacking
Come indicato al punto 5.1.1, la struttura informatica e sistemistica del Fornitore rende improbabile tale rischio (firewall, collegamento vpn).

5.2.3 Evento esterno
Eventi esterni, per quanto improbabili, si possono superare ricorrendo alle copie di backup che vengono eseguite quotidianamente e mantenute per 7 giorni.

6. Parere delle parti interessate

Non è stato richiesto un parere alle parti interessate in quanto la finalità del trattamento rappresentano l'adempimento di obblighi di legge. Ai fini dell'attivazione del canale di segnalazione interna, gli enti devono sentire le rappresentanze o le organizzazioni sindacali.

7. Parere DPO

Il DPO esprime il proprio parere favorevole alla DPIA effettuata con riferimento alla valutazione di impatto dei dati personali relativi agli adempimenti in materia di whistleblowing, in quanto conformi al dettato normativo.

8. Conclusioni

Dall'analisi sull'impatto dei rischi valutati in particolare nell'ambito dei trattamenti individuati aventi l'obbligo di DPIA, emergono rischi residui con impatto sui diritti e libertà degli interessati con stima a valore basso.

Considerando le attività di mitigazione dei rischi messe in atto da Responsabile e Sub-Responsabile si ritiene che i rischi del trattamento preso in considerazione siano da considerarsi bassi.

Considerando che il trattamento è obbligatorio e che il grado di rischio sui diritti e libertà dell'interessato è basso, si ritiene non necessaria una consultazione preventiva all'Autorità Garante.

Si potrà quindi procedere con il trattamento a condizione di rivalutare la presente DPIA ogni qualvolta dovesse modificare una o più informazioni che la riguardano e comunque almeno una volta all'anno per controllare che non siano intervenute modifiche alla presente analisi.

Si allega il documento "DOCUMENTAZIONE A SUPPORTO DEL TITOLARE PER LA VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI".

Borgo San Lorenzo, lì _____

_____