Comune di Sassofeltrio

Provincia di Rimini

Valutazione di impatto

Trattamento dati relativi alle segnalazioni di
Condotte illecite (c.d. whistleblowing)

(***D.P.I.A.*** - Data Protection Impact Assessment o ***P.I.A.*** - Privacy Impact Analysis)

Articolo 35 del Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)

Articolo 13, comma 6, del DECRETO LEGISLATIVO 10 marzo 2023, n. 24

Il documento è stato redatto, con la collaborazione del RPD, in data 10/04/2025.
Approvato con deliberazione di Giunta Comunale n30 in data 18/04/2025.

Responsabile della Protezione dei Dati (RPD-DPO)

Gruppo Gaspari – Servizio privacy

Siamo contattabili

Via e-mail: privacy@gaspari.it

Via PEC: privacy@pec.egaspari.net

Via Posta ordinaria: Grafiche E.Gaspari Srl, Via M. Minghetti - 18, 40057, Cadriano di Granarolo Emilia (Bologna)

Via telefono: 051-763201

1. Cos'è la valutazione di impatto

(D.P.I.A. - Data Protection Impact Assessment o P.I.A. - Privacy Impact Analysis)

1.1. Premesse normative

Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)

Articolo 35 Valutazione d'impatto sulla protezione dei dati

1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. ***Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi***.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) *una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;*

b) *il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o*

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68[1].

---

[1] *Il Garante della Privacy italiano ha emanato un "**Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679 - 11 ottobre 2018** - (Pubblicato sulla Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018)" - In questo elenco sono previste le seguenti fattispecie:*

- *Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato".*
- *Trattamenti automatizzati finalizzati ad assumere decisioni che producono "effetti giuridici" oppure che incidono "in modo analogo significativamente" sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).*
- *Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc.*

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene almeno:

a) *una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*

b) *una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*

c) *una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*

d) *le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.*

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

---

effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.

- *Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).*
- *Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).*
- *Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).*
- *Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01 .*
- *Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.*
- *Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment).*
- *Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.*
- *Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*
- *Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.*

9. Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

10.Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e)[2], trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, ***i paragrafi da 1 a 7 non si applicano***, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.

11. Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.

[2] ***Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)***

Articolo 6 Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni:
[…]
c) il trattamento ***è necessario per adempiere un obbligo legale*** *al quale è soggetto il titolare del trattamento; […]*
e) il trattamento ***è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento****; (C45, C46)*

1.2. Premesse metodologiche

Il Garante della Privacy italiano, ha messo a punto un opuscolo che tra le altre cose [*https://www.garanteprivacy.it/documents/10160/0/Infografica+-+Valutazione+d+impatto+sulla+protezione+dei+dati++-+DPIA.pdf/13477c9e-1e81-4edc-9fa3-4ccf8e7b0e6d?version=1.3*] prevede:

> "*La DPIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali. Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego per tutti i trattamenti, e non solo nei casi in cui il Regolamento la prescrive come obbligatoria.*"

A tal fine ha collaborato con il Garante della Privacy Francese per mettere a punto un software open source, simili a quello che hanno messo in commercio diverse aziende private; nella pagina download [https://www.garanteprivacy.it/regolamentoue/DPIA#STRUMENTI] del software ha premesso:

> *"Il software qui presentato NON costituisce un modello al quale fare riferimento in ogni situazione di trattamento, essendo stato concepito soprattutto come ausilio metodologico per le PMI. Offre in ogni caso un focus sugli elementi principali di cui si compone la procedura di valutazione d´impatto sulla protezione dei dati. Potrebbe costituire quindi* ***un utile supporto di orientamento allo svolgimento di una DPIA****, ma non va inteso come schema predefinito per ogni valutazione d´impatto che va integrata in ragione delle tipologie di trattamento esaminate.*
>
> *E´ inoltre bene ricordare che la valutazione d´impatto sulla protezione dei dati deve tenere conto del rischio complessivo che il trattamento previsto può comportare per i diritti e le libertà degli interessati, alla luce dello specifico contesto. Pertanto, il concetto di rischio non si esaurisce nella considerazione delle possibili violazioni o minacce della sicurezza dei dati."*

1.3. Individuazione e gestione del rischio

Per valutare quali rischi corrono i dati personali dei cittadini che vengono trattati dal titolare e dal responsabile del trattamento, bisogna individuare una serie di elementi che il Garante della Privacy italiano ha messo a fuoco in alcune diapositive pubblicate sul suo sito e che riproduciamo in parte qui di seguito

[https://www.garanteprivacy.it/documents/10160/0/Individuazione+e+gestione+del+rischio+-+Tutorial+-+slide.pdf/d2eb9375-c577-4ff3-b716-38cc703ec26f?version=1.0]:

ATTENZIONE!

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Aspetti riguardanti la sicurezza del trattamento

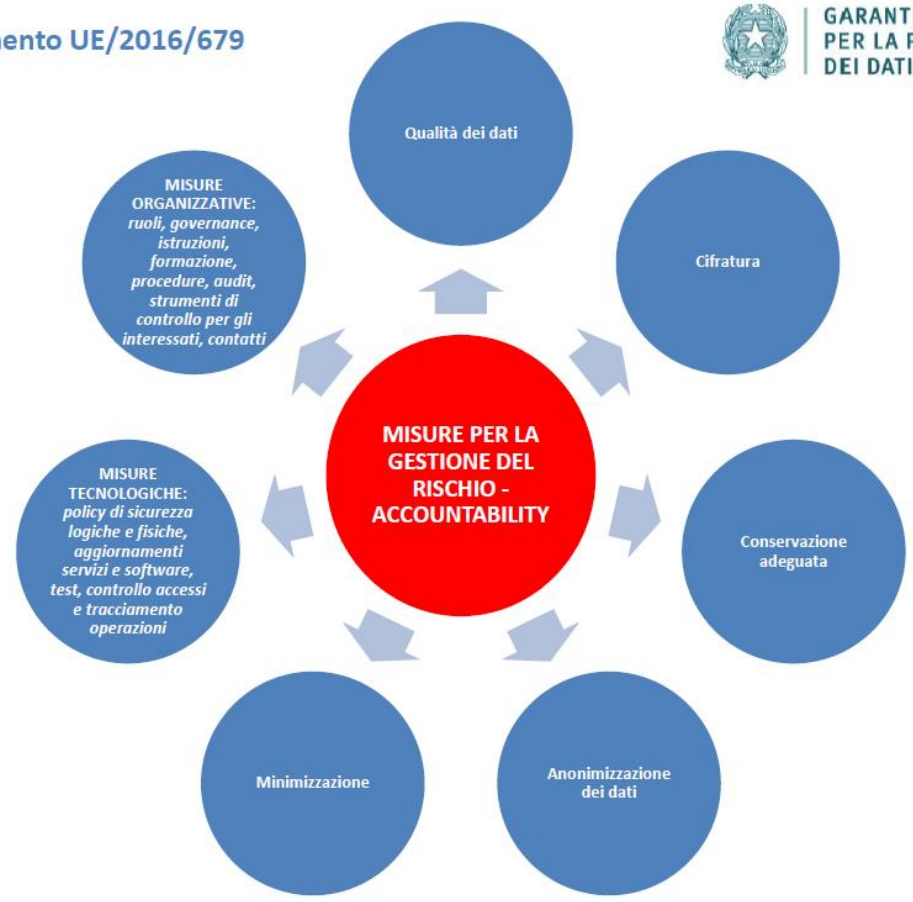
- **DISPONIBILITÀ**
  -distruzione
  -indisponibilità
  -perdita
- **INTEGRITÀ**
  -alterazione
- **RISERVATEZZA**
  -divulgazione
  -accesso

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI



1.4. La valutazione di impatto per un comune, modalità

Abbiamo visto in queste premesse normative e metodologiche quattro elementi fondamentali e parzialmente contraddittori, ancora non chiariti né dal Garante né dalla dottrina, che faticosamente sta cercando di assestarsi:

1. *Quando un trattamento di dati è massivo, come quello effettuato da un comune, sembrerebbe obbligatorio fare la PIA*
2. *Quando però un trattamento di dati è previsto e disciplinato da norme imperative o è effettuato nell'ambito di un pubblico interesse, come tutti i trattamenti di dati del comune, sembrerebbe escluso che debba essere sottoposto a PIA*
3. *I prodotti informatici in commercio e il software open source del Garante non sono predisposti per i comuni, ma per le piccole e medie imprese;*
4. *Sembra opportuno in questa prima fase di applicazione del RGPD, effettuare comunque una PIA anche se non obbligati*

Ciò premesso, il legislatore può individuare specifici trattamenti che richiedono una valutazione d'impatto.

È il caso del trattamento dati relativi alle segnalazioni di Condotte illecite (c.d. whistleblowing).

DECRETO LEGISLATIVO 10 marzo 2023, n. 24

Art. 13, comma 6

6. I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, ***individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione d'impatto sulla protezione dei dati****, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del regolamento (UE) 2016/679 o dell'articolo 18 del decreto legislativo n. 51 del 2018.*

Di seguito effettuiamo una PIA, utilizzando gli strumenti di misurazione illustrati nelle slide e nel software opportunamente adattata ad una serie di trattamenti molto diversi, sia come metodologia che come base giuridica, rispetto a quelli delle PMI

1.5. Descrizione del Sistema adottato

Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio.

ARCHITETTURA DI SISTEMA

L'architettura di sistema è principalmente composta da:

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

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software libero ed open-source **GlobaLeaks** di cui Whistleblowing Solutions è co-autore e coordinatore di progetto.

In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile.

Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- VMware, software di virtualizzazione;
- Veeam, software di backup;
- Plesk, software per realizzazione siti web di facciata del progetto.

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.

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 1.2+;
- Ogni macchina virtuale istanziata vede esposizione di rete limitata all’effettiva necessità;
- 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.

1.6. Analisi del contesto

Responsabilità connesse al trattamento	**PA, Ente o Organizzazione** > Titolare del trattamento **Gestore delle segnalazioni** > Soggetto autorizzato dal Titolare del Trattamento a trattare i dati relativi alle segnalazioni **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) **Transparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Standard applicabili	Il contesto normativo di riferimento richiede conformità 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

Dati e operazioni di trattamento	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.
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 per finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore
Risorse a supporto delle attività di trattamento	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)

2. Risultati della rilevazione per la valutazione di impatto

Art. 35 del Regolamento generale per la protezione dei dati

(RGPD - REGOLAMENTO - UE - 2016/679)

Sezione 1: adempimenti di carattere generale

1. **E' stato nominato un Responsabile della protezione dei dati?**

   Sì, con apposito atto

Punti 6 (*Sì= 6 – No = 0*)

2. **E' stata fatta la comunicazione al Garante della Privacy della nomina del RPD?**

   Sì, in data 11/03/2022

Punti 6 (*Sì= 6 – No = 0*)

3. **I dati di contatto del RPD sono presenti sul sito istituzionale?**

   Si

Punti 6 (*Sì= 6 – No = 0*)

4. **I dati di contatto del RPD sono presenti sulle informative?**

   Si

Punti 6 (*Sì= 6 – No = 0*)

5. **E' stato adottato un Registro dei trattamenti?**

   Sì, l'Ente ha adottato un Registro dei trattamenti. L'attuale registro è in fase di revisione per un opportuno aggiornamento.

Punti 3 (*Sì= 6 – No = 0*)

Tot. punti sez.1: 27

Sezione 2: - mappatura del rischio

6. Mappatura del Rischio Trattamento dati relativi alle segnalazioni di condotte illecite (c.d. whistleblowing)

COD.	Denominazione della banca dati personale	**Massimo 30 punti**

Il punteggio max di 30 si ottiene solo se il servizio è gestito direttamente dal comune, sommando questi elementi:

- *Max 10 se la banca dati è gestita in formato elettronico con apposito applicativo*
- *Max 10 se l'applicativo risponde a criteri di affidabilità*
- *Max 10 se gli operatori impiegati sono adeguatamente formati*

Banche dati personali dei servizi di vigilanza e controllo	
Whistleblowing	
Criteri	Punteggio
Banca dati è gestita in formato elettronico con apposito applicativo	10
L'applicativo risponde a criteri di affidabilità	10
Gli operatori impiegati sono adeguatamente formati	8

Massimo 30 punti

Tot. punti sez. 2: 28

Sezione 3: misure di sicurezza logiche

7. Sono state adottate queste misure “logiche” di sicurezza per gli archivi informatici

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

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 parte dell’applicativo delle funzionalità sicurezza del database e delle policy di data retention e cancellazione sicura.

GESTIONE DELLE VULNERABILITÀ TECNICHE

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 ireport 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

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

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.

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.

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.

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.

Tot. punti sez. 3: 30

Sezione 4: - gestione del dato e tutela dei diritti degli interessati

8. L'assetto attuale delle misure adottate

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)

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.

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.

Esattezza e aggiornamento dei dati

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.

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.

Definizione degli obblighi dei responsabili del trattamento e formalizzazione dei contratti

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

Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:

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.

Tot. punti sez. 5: 30

La rilevazione dei dati e l'assegnazione **provvisoria** dei punteggi è stata eseguita da:

Segretario Comunale Dott.ssa Valentina Zangheri in data 08/04/2025

Dopodiché i dati rilevati sono stati trasmessi al RPD, che ha assegnato i relativi punteggi **finali**.

3. Risultati e prescrizioni della valutazione di impatto

3.1. Tabella riassuntiva (riportare i punteggi di ciascuna sezione):

Sez.	Denominazione della sezione	Punti
1	***adempimenti di carattere generale***	27
2	***mappatura del rischio***	28
3	***misure di sicurezza logiche***	30
4	***gestione del dato e tutela dei diritti degli interessati***	30
Totale punteggio (somma da 1 a 5)		100/120

3.2. Panoramica dei rischi e possibili impatti

	Accesso illegittimo ai dati	**Modifiche indesiderate dei dati**	**Perdita di dati**
Principali impatti sugli interessati se il rischio si dovesse concretizzare	Diffusione non autorizzata, intercettazione di informazioni in rete, danno alla reputazione e all'onore	Alterazione dei dati, negazione dell'accesso a servizi, danno alla reputazione e all'onore	Indisponibilità dei dati, danno reputazionale
Principali minacce che potrebbero concretizzare il rischio?	Virus (malware), Accesso non autorizzato alla rete, Trattamento (volontario o inconsapevole) non consentito di dati (personali), Uso dei servizi da parte di persone non autorizzate, Uso di servizi in modo non autorizzato, intercettazione (inclusa analisi del traffico), Rivelazione di informazioni (da parte del personale o fornitori), Infiltrazione nelle comunicazioni, Uso non autorizzato della strumentazione	Accesso non autorizzato alla rete, Infiltrazione nelle comunicazioni, Uso dei servizi da parte di persone non autorizzate, Uso di servizi in modo non autorizzato, Uso non autorizzato della strumentazione, Virus (malware)	Accesso non autorizzato alla rete, Uso dei servizi da parte di persone non autorizzate, Uso di servizi in modo non autorizzato, Uso non autorizzato della strumentazione, Virus (malware)
Fonti di rischio	Infrastruttura informatica, modalità di detenzione credenziali, non adeguata formazione del personale che deve trattare i dati, accesso non autorizzato alla strumentazione, azienda di manutenzione non adeguatamente responsabilizzata ed istruita	Accesso non autorizzato alla strumentazione, infrastruttura informatica, azienda di manutenzione non adeguatamente responsabilizzata ed istruita, modalità di detenzione credenziali, non adeguata formazione del personale che deve trattare i dati	Accesso non autorizzato alla strumentazione, azienda di manutenzione non adeguatamente responsabilizzata ed istruita, infrastruttura informatica, modalità di detenzione credenziali, non adeguata formazione del personale che deve trattare i dati

Misure, fra quelle individuate, che contribuiscono a mitigare il rischio	Controllo degli accessi logici, Crittografia, Tracciabilità, Archiviazione, Vulnerabilità, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro il malware	Crittografia, Controllo degli accessi logici, Tracciabilità, Vulnerabilità, Backup, Sicurezza dei canali informatici, Manutenzione, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Archiviazione, Lotta contro il malware	Controllo degli accessi logici, Archiviazione, Vulnerabilità, Backup, Manutenzione, Sicurezza dei canali informatici, Sicurezza dell'hardware, Lotta contro il malware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali
Gravità	**Medio**	**Medio**	**Limitato**
Probabilità	**Trascurabile**	**Trascurabile**	**Trascurabile**

3.3. Valutazione d'impatto in relazione ai rischi e alle misure adottate

Misure da adottare	***Valutazione di impatto*** (*rappresentazione grafica*)
Se il punteggio della sezione è in questo spazio la situazione è sicura, ma serve vigilare per mantenere i risultati raggiunti	**Da 25 a 30**
Se il punteggio della sezione è in questo spazio la situazione è già accettabile, ma conviene agire su qualche misura, per consolidare	**Da 19 a 24**
Se il punteggio della sezione è in questo spazio è utile agire su qualcuna delle misure	**Da 13 a 18**
Se il punteggio della sezione è in questo spazio è necessario agire sulla maggior parte delle misure	**Da 7 a 12**
Se il punteggio della sezione è in questo spazio è necessario agire su tutte le misure previste	**Da 0 a 6**

Gradazione del rischio	Rischio massimo	Rischio elevato	Rischio medio	Rischio Limitato	Rischio Trascurabile

3.4. Prescrizioni del "validatore" :

Dall'analisi della rilevazione e dall'esplicazione dei punteggi ottenuti si ritiene necessario prescrivere (per ciascuna sezione):

Sez.	Denominazione della sezione
1	***Adempimenti di carattere generale***
Prescrizioni per l'abbattimento del rischio: La maggior parte degli adempimenti di carattere generale sono stati attuati. Tuttavia, si raccomanda un tempestivo aggiornamento del Registro dei Trattamenti, ex articolo 30 del GDPR, come da indicazioni già fornite da questo RPD	
2	***mappatura del rischio***
Prescrizioni per l'abbattimento del rischio: Sono state prese cautele adeguate per ridurre il rischio connesso al trattamento dei dati di cui alla presente DPIA. La raccomandazione è quella di prevedere ogni anno una formazione sempre aggiornata in materia di anticorruzione, così come previsto dalla legge 190/2012 (all'art. 1, co. 9, lett. b)))	
3	***misure di sicurezza logiche***
Prescrizioni per l'abbattimento del rischio: La strumentazione software adottata sembra assicurare un elevato grado di sicurezza.	
4	***gestione del dato e tutela dei diritti degli interessati***
Prescrizioni per l'abbattimento del rischio: Le policy di gestione del dato risultano ideonee. L'Ente ha pubblicato un'informativa adeguata, e sono stati ben configurati i rapporti con il fornitore del software tramite un'apposita nomina a Responsabile del Trattamento ex art. 28 del GDPR	