

DPIA

GESTIONE DELLE SEGNALAZIONI DI CONDOTTE ILLECITE (WHISTLEBLOWING)



Autore

Comune di Urganano

Nome del DPO/RPD

Privacycert Lombardia S.r.l. – Referente dott. Massimo Zampetti

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

I rischi residui, a seguito delle misure di sicurezza intraprese, sono congrui alle finalità del trattamento.

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non si è ritenuto necessario richiedere un parere agli interessati. Qualora vi fossero suggerimenti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto degli stessi.

CONTESTO

La tabella seguente mostra le informazioni di base della DPIA:

TABELLA 1	
DESCRIZIONE E SCOPO DELLA DPIA	La presente valutazione di impatto è effettuata dal Comune allo scopo di valutare l'impatto sui diritti e libertà dei soggetti segnalanti un illecito di interesse generale nell'ambito dell'amministrazione pubblica. In attuazione della Direttiva (UE) 2019/1937, emanato il d.lgs. n. 24 del 10 marzo 2023 riguardante <i>"la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali"</i> , si è ritenuto opportuno svolgere una valutazione di impatto sui potenziali rischi connessi alla gestione delle segnalazioni pervenute al Comune su piattaforma dedicata (Whistleblowing.it).
PERSONE INTERESSATE E TIPOLOGIE DI DATI PERSONALI TRATTATI	I dati personali oggetto di trattamento sono i dati del "Segnalante", del "Segnalato" e delle persone coinvolte e/o collegate ai fatti oggetto della Segnalazione"
FINALITÀ DEL TRATTAMENTO	I dati personali sono trattati, nell'ambito del procedimento di "Whistleblowing", esclusivamente per le finalità di istruttoria ed accertamento dei fatti oggetto della Segnalazione e di adozione degli eventuali conseguenti provvedimenti.
MINIMIZZAZIONE E AGGIORNAMENTO DEI DATI	i dati personali raccolti sono solo quelli necessari e pertinenti per il raggiungimento delle finalità sopra indicate, sulla base del "principio di minimizzazione", ai sensi dell'art. 5.1 lett. C) GDPR. Rispetto a questi dati, il loro conferimento è volontario e l'Interessato è pregato di fornire soltanto i dati necessari a descrivere i fatti oggetto della Segnalazione senza comunicare dati personali ridondanti ed ulteriori a quelli necessari rispetto alle finalità sopra indicate. Nel caso siano forniti, tali dati non saranno utilizzati.
PERIODO DI CONSERVAZIONE DEI DATI	I dati personali saranno conservati solo per il tempo necessario alle finalità per le quali vengono raccolti nel rispetto del principio di minimizzazione ex art. 5.1.c) GDPR e, in particolare, alle finalità di gestione dell'istruttoria, di conclusione dell'attività di definizione della Segnalazione e di adozione dei relativi provvedimenti, in caso di accertamento. Il software web based in uso (piattaforma informatica di segnalazione basata sul software libero ed open-source GlobalLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto) indica nella sua policy di data retention, un tempo di conservazione delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.
MODALITÀ DI INFORMAZIONE ADOTTATA	Informativa ai sensi dell'art. 13 del GDPR disponibile sulla pagina privacy policy del sito web del Comune. Nel modulo di segnalazione si richiede presa visione del testo informativo con link di rimando alla pagina dedicata. Sono inoltre fornite le istruzioni operative per procedere alla segnalazione, qualora sia interna.
DESTINATARI DEI DATI TRATTATI	I dati personali e quelli delle persone indicate come possibili responsabili delle condotte illecite, nonché delle persone a vario titolo coinvolte nelle vicende segnalate, non saranno oggetto di diffusione, tuttavia, se necessario, su loro richiesta, possono essere trasmessi all'Autorità Giudiziaria, alla Corte dei conti e all'ANAC, Autorità nazionale anticorruzione. Tali soggetti sono, tutti, Titolari autonomi del trattamento.
COMUNICAZIONE DATI AL DI FUORI DELL'UE	I dati personali non sono oggetto di trasferimento al di fuori dell'Unione Europea.

VALUTAZIONE PRELIMINARE

Il Titolare del trattamento, con il supporto del Responsabile per la protezione dati, ha effettuato una analisi preliminare sulla necessità o meno di condurre una **Valutazione di Impatto (DPIA – “Data Protection Impact Assessment”)** sulla **protezione dei dati personali**, adottando come guida la Tabella 2 seguente, tratta dai “criteri da considerare secondo il Gruppo di Lavoro Art. 29 (WP 29)”.

Criteri da considerare secondo il gruppo di lavoro art. 29 (wp 29) quando si identifica un rischio elevato (che richiede l'impegno di una DPIA).

I TRATTAMENTI SONO RIFERITI AI SEGUENTI CRITERI?	SI	NO
1. Valutazione o punteggio, inclusa la profilazione e la previsione		X
2. Processo decisionale automatizzato con effetto significativo legale o simile		X
3. Monitoraggio sistematico (es. videosorveglianza su larga scala)		X
4. Dati sensibili, giudiziari, etc.	X	
5. Dati trattati su larga scala		X
6. Set di dati che sono stati abbinati o combinati		X
7. Dati riguardanti soggetti vulnerabili (es. minori, dipendenti ecc...)	X	
8. Uso innovativo o applicazione di soluzioni tecnologiche o organizzative (es: riconoscimento facciale, ecc...)		X
9. Quando l'elaborazione in sé "impedisce agli interessati di esercitare un diritto o di utilizzare un servizio o un contratto (es: selezione clienti banca per concessione finanziamento)		X

Il Gruppo di Lavoro Art. 29 suggerisce di effettuare una DPIA se almeno 2 (due) dei criteri di cui sopra sono soddisfatti. La valutazione preliminare conferma quindi che almeno due criteri della tabella precedente sono soddisfatti, pertanto il Titolare del trattamento, con il supporto del Responsabile per la protezione dei dati, ha ritenuto di effettuare una esaustiva **Valutazione di Impatto (DPIA) sulla protezione dei dati personali**, con l'impegno di rivederla periodicamente (in caso di variazione significativa dei dati trattati o del loro trattamento o almeno con cadenza annuale).

PANORAMICA DEL TRATTAMENTO

Quale è il trattamento in considerazione?

Il trattamento è finalizzato alla corretta e completa gestione delle segnalazioni - incluse le eventuali attività di indagine necessarie a valutarne la fondatezza - trasmesse dal segnalante in riferimento alle "Istruzioni per la segnalazione delle violazioni" adottate dal Comune in ottemperanza a quanto previsto dalla normativa vigente (L.179 del 2017; art. 54 bis del d.lgs. 165/2001; D. Lgs. n. 24 del 10 marzo 2023, di attuazione della Direttiva (UE) 2019/1937).

I dati personali sono trattati dal Titolare del trattamento e dal Responsabile della prevenzione della corruzione e della trasparenza nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità dell'Ente, ai sensi dell'art. 54-bis del d.lgs. n. 165/2001, dai soggetti che, in ragione del proprio rapporto di lavoro presso l'Ente, vengano a conoscenza di condotte illecite, in particolare: il Segretario Comunale, il Sindaco; i dipendenti di ruolo e a tempo determinato; le persone addette all'ufficio o i consulenti; i dipendenti di altre amministrazioni in posizione di comando, distacco o fuori ruolo presso l'Ente; i lavoratori e i collaboratori delle imprese fornitrici di beni o servizi presso l'Ente.

COMUNE DI URGNANO (BG)

Il Comune si è dotato di una piattaforma web based per le segnalazioni di illecito.

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.

Quali sono le responsabilità connesse al trattamento?

- **PA, Ente o Organizzazione** > Titolare 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)
- **Transparency 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?

- 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?

La piattaforma Whistleblowing.it in uso presso il Comune raccoglie e conserva i 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)?

- 1) Attivazione della piattaforma di segnalazione "Whistleblowing.it"
- 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

Quali sono le risorse di supporto ai dati?

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)

COMUNE DI URGNANO (BG)

- OPENVPN (vpn)

Valutazione: Accettabile

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati che il Comune richiede tramite registrazione sulla piattaforma di segnalazione sono acquisiti allo scopo di procedere all'accertamento dei fatti segnalati e adottare eventuali provvedimenti. Ai sensi dell'art. 6, comma 1 lettera f) del Regolamento Europeo n. 679/2016, tutti i dati personali raccolti nell'ambito del trattamento in oggetto sono strettamente funzionali e necessari per il perseguimento del legittimo interesse del titolare medesimo.

Il conferimento dei dati necessari al perseguimento delle finalità del Titolare (dati obbligatori in caso di segnalazione in forma non anonima) ha natura "obbligatoria" ed un eventuale rifiuto comporta l'impossibilità per il Comune di ricevere la segnalazione.

I dati facoltativi eventualmente forniti sono trattati esclusivamente ai fini di una migliore gestione della segnalazione. In particolare, i dati di contatto sono utilizzati solo nel caso in cui dovesse rendersi necessario un contatto diretto con il segnalante.

Valutazione: Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

Tenuto conto della normativa di riferimento e, in particolare, dell'art. 54-bis D.lgs. 165/2001, si precisa che:

- il trattamento dei dati "comuni" si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR), nonché sull'esecuzione di compiti di interesse pubblico assegnati dalla legge all'Agenzia delle entrate (art. 6, par. 1, lett. e) del GDPR);
- il trattamento di dati "particolari" si fonda sull'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'Interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), GDPR), nonché sull'esecuzione di un compito di interesse pubblico rilevante assegnato dalla legge al Comune (art. 9, par. 2, lett. g), GDPR), in ragione dell'art. 2-sexies lett. dd) del D.lgs. 196/2003;
- il trattamento di dati relativi a condanne penali e reati, tenuto conto di quanto disposto dall'art. 10 GDPR, si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), GDPR) e sull'esecuzione di compiti di interesse pubblico assegnati dalla legge (art. 6, par. 1, lett. e), GDPR), in ragione dell'art. 2-octies lett. a) del D.lgs. 196/2003.

Si precisa che, in ragione di quanto disposto dall'art. 54-bis D.lgs. 165/2001, nel caso in cui la segnalazione portasse all'instaurazione di un procedimento disciplinare nei confronti del responsabile della condotta illecita, l'identità del segnalante non verrà mai rivelata. Qualora la conoscenza dell'identità del segnalante fosse indispensabile per la difesa dell'incolpato, verrà domandato al segnalante se intende rilasciare un apposito, libero consenso ai fini della rivelazione della propria identità.

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)?

Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, E-mail 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 GlobalLeaks, 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 GlobalLeaks 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?

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?

Policy di data retention di default delle segnalazioni di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute. La proroga della scadenza può essere fatta dal soggetto ricevente più volte.

Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio, a condizione che non esistano segnalazioni aperte sulla piattaforma.

Valutazione: Accettabile

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati vengono informati attraverso la predisposizione di un documento informativo ai sensi dell'art. 14 del reg. EU 679/2016 pubblicato sul sito web istituzionale e indicata una dicitura di presa visione nel modulo di segnalazione.

Valutazione: Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non costituisce una base giuridica idonea per il trattamento dei dati e quindi non è richiesto per la procedura di segnalazione.

Ciononostante, in ragione di quanto disposto dall'art. 54-bis D.lgs. 165/2001, nel caso in cui la segnalazione portasse all'instaurazione di un procedimento disciplinare nei confronti del responsabile della condotta illecita, l'identità del segnalante non verrà mai rivelata. Qualora la conoscenza dell'identità del segnalante fosse indispensabile per la difesa dell'incolpato, verrà domandato al segnalante se intende rilasciare un apposito, libero consenso ai fini della rivelazione della propria identità

Valutazione: Accettabile

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Valutazione: Accettabile

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Valutazione: Accettabile

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

Gli interessati possono sempre rivolgersi ai contatti presenti nell'informativa per l'esercizio dei propri diritti.

Valutazione: Accettabile

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

Gli accordi contrattuali sono definiti con le seguenti società:

- Whistleblowing Solutions in qualità di Responsabile del trattamento

COMUNE DI URGNANO (BG)

- 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

COMUNE DI URGNANO (BG)

L'applicativo GlobalLeaks 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 SSL Labs 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 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

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

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.

Valutazione: Accettabile

Archiviazione

L'applicativo GlobalLeaks 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.

COMUNE DI URGNANO (BG)

Valutazione: Accettabile

Gestione delle vulnerabilità tecniche

L'applicativo GlobalLeaks 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

Manutenzione

È prevista manutenzione periodica correttiva, evolutiva e con finalità di migloria 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

Controllo degli accessi fisici

Gli accessi agli uffici amministrativi sono limitati al personale autorizzato. Nessun soggetto terzo può accedere, se non previa autorizzazione unicamente per le sole finalità connesse all'incarico assunto (es. manutenzione ecc.).

Il plesso scolastico dove si trovano gli uffici amministrativi e di segreteria sono regolarmente presidiati dal personale in servizio al fine di accogliere l'utenza in ingresso.

Valutazione: Accettabile

Sicurezza dell'hardware

Tutte le connessioni sono protette tramite protocollo TLS 1.2+

Le connessioni amministrative privilegiate sono mediate tramite accesso VPN e connessioni con protocollo SSH.

Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Valutazione: Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

COMUNE DI URGNANO (BG)

Whistleblowing Solutions ha definito una procedura per la gestione delle violazioni dei dati personali.

Valutazione: Accettabile

Lotta contro i 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.

Misure aggiuntive

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.

A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:

- THREAT MODEL
- APPLICATION SECURITY

Valutazione: Accettabile

RISCHI

Accesso illegittimo ai dati

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

COMUNE DI URGNANO (BG)

Ritorsione, Uso improprio di dati personali, Valutazioni Errate, Danno Reputazionale

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Mancata formazione, Sottovalutazione del Rischio, Comportamento negligente

Quali sono le fonti di rischio?

fonti non umane, fonti umane interne, fonti umane esterne

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo accessi logici, Backup, Tracciabilità, Archiviazione, Gestione delle vulnerabilità tecniche, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro i malware, Misure aggiuntive

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

Limitata, Limitato

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

Limitata, Limitato

Valutazione: Accettabile

RISCHI

Modifiche indesiderate dei dati

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

COMUNE DI URGNANO (BG)

Danno Reputazionale, Ritorsione, Uso improprio di dati personali, Valutazioni Errate

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

Comportamento negligente, Mancata formazione, Sottovalutazione del Rischio, Attività Fraudolenta

Quali sono le fonti di rischio?

fonti non umane, fonti umane esterne, fonti umane interne

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

Crittografia, Controllo accessi logici, Backup, Tracciabilità, Archiviazione, Gestione delle vulnerabilità tecniche, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro i malware, Misure aggiuntive

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

Limitata, Limitato

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

Limitata, Limitato

Valutazione: Accettabile

RISCHI

Perdita di dati

COMUNE DI URGNANO (BG)

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

Ritorsione, Uso improprio di dati personali, Danno Reputazionale

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

Mancata formazione, Comportamento negligente, Sottovalutazione del Rischio, Attività Fraudolenta

Quali sono le fonti di rischio?

fonti non umane, fonti umane esterne, fonti umane interne

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

Crittografia, Controllo accessi logici, Backup, Tracciabilità, Archiviazione, Gestione delle vulnerabilità tecniche, Manutenzione, Controllo degli accessi fisici, Sicurezza dell'hardware, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Lotta contro i malware, Misure addizionali

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

Limitata, Limitato

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

Limitata, Limitato

Valutazione: Accettabile

RISCHI - PANORAMICA DEI RISCHI

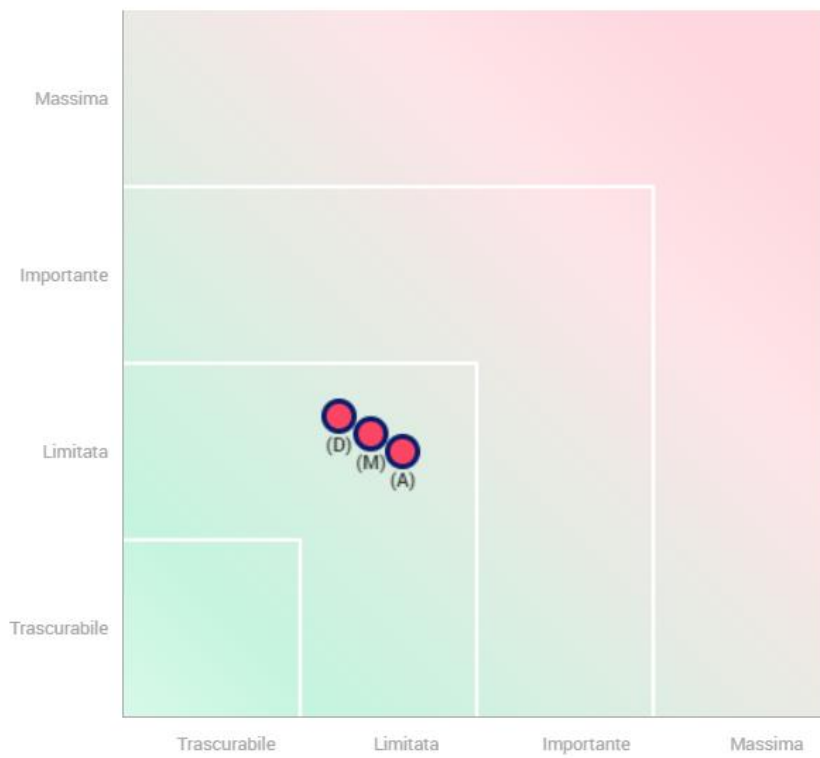


COMUNE DI URGNANO (BG)

MAPPATURA DEL RISCHIO

COMUNE DI URGNANO (BG)

Gravità del rischio



Probabilità del rischio

- **Misure pianificate o esistenti**
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati