COMUNE DI GABBIONETA BINANUOVA
Provincia di Cremona

DPIA

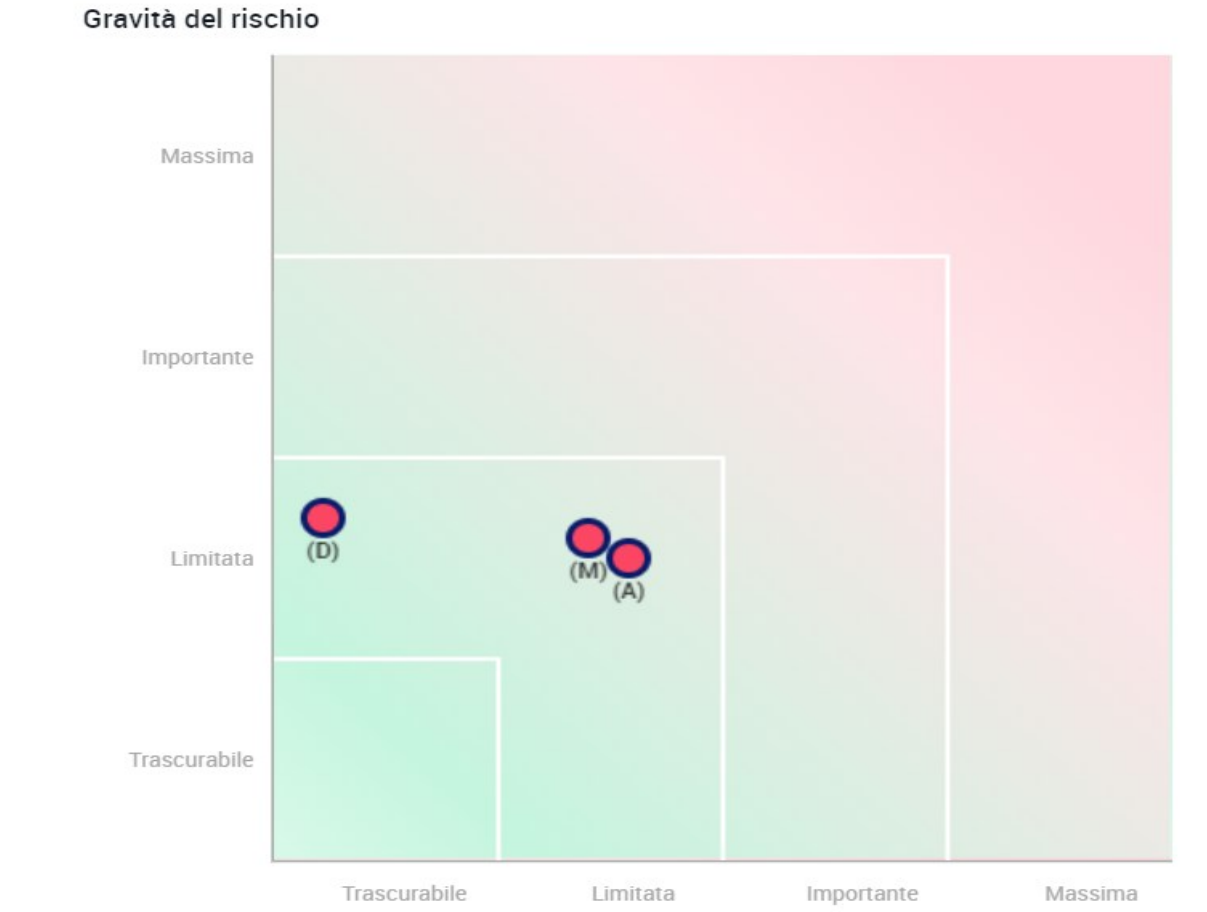
RELATIVA ALL'INTRODUZIONE DI UNA PIATTAFORMA PER IL WHISTLEBLOWING

WHISTLEBLOWING SOLUTIONS

(MEDIANTE UTILIZZO DEL SOFTWARE P.I.A.)

Approvato con Deliberazione di Giunta n. _____ del ____/____/2023

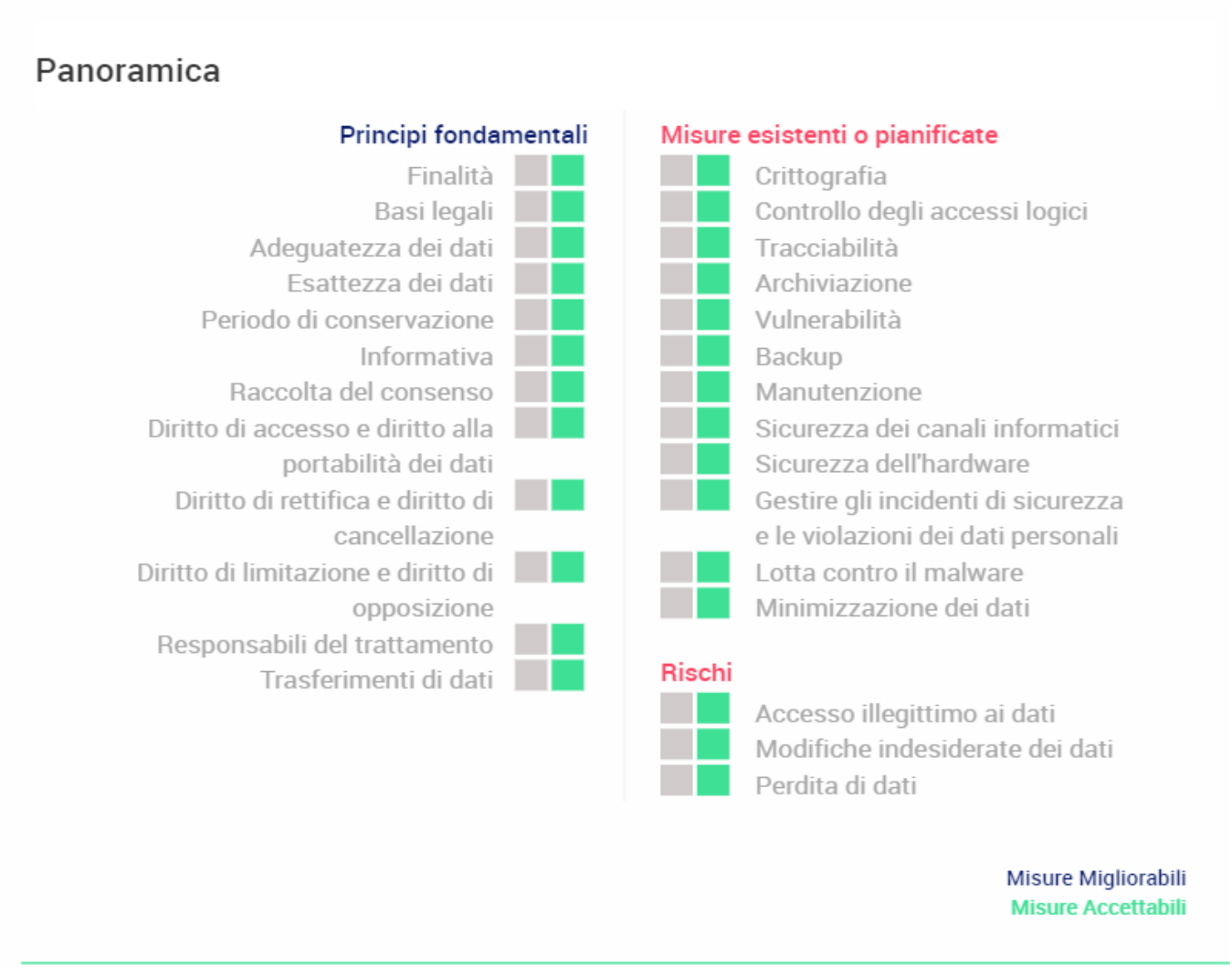
MAPPATURA DEL RISCHIO



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

18/07/23

PIANO D'AZIONE DEL RISCHIO



CONTESTO

Panoramica del trattamento

Il trattamento di cui alla presente DPIA riguarda l'introduzione di una piattaforma per le segnalazioni di illeciti di interesse generale nell'ambito del contesto lavorativo. Il **decreto legislativo n. 24/2023**, che introduce la nuova disciplina del **whistleblowing** in Italia, è entrato in vigore il 30 marzo 2023. Il provvedimento, attuativo della **direttiva europea 2019/1937**, raccoglie in un unico testo normativo l'intera disciplina dei canali di segnalazione e delle tutele riconosciute ai segnalanti, sia del settore pubblico che privato. Il Comune ha deciso di introdurre il proprio canale di segnalazioni interne avvalendosi di **WhistleblowingPA,** un progetto di **Transparency International Italia** e di **Whistleblowing Solutions Impresa Sociale**.

Le figure soggettive connesse al trattamento

Titolare del Trattamento è il Comune di Gabbioneta Binanuova (PI 00325740199) nella persona del Sindaco pro tempore. La sede legale è in Via della Libertà, 5, 26030 Gabbioneta Binanuova, pec: comune.gabbioneta-binanuova@pec.regione.lombardia.it, tel: 0372 844314.

Responsabile Esterno del Trattamento è Whistleblowing Solutions I.S. S.r.l., con sede in Viale Abruzzi 13/A, 20131, Milano, Codice Fiscale e P. IVA 09495830961 del legale rappresentante pro tempore Ing. Giovanni Pellerano. Nominato dal Sindaco con accordo in data 24.07.2023 e trasmesso nella medesima data.

Data Protection Officer è Avv. Alessia Roberto, Via Sauli n. 39/11, Genova (GE) che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente indirizzo e-mail aroberto.legale@gmail.com.

Incaricato del trattamento, per espressa previsione di legge, in quanto Responsabili della Prevenzione della Corruzione e Trasparenza è il Segretario del Comune di Gabbioneta Binanuova, Dott.ssa Giovanna Tomasoni, in quanto persona fisica avente l'accesso esclusivo all'indirizzo e-mail al quale pervengono tutte le segnalazioni.

Gli standard applicabili al trattamento

Al trattamento in si applicano le seguenti **normative e provvedimenti**:

- Regolamento UE n. 2016/679 (GDPR);

- D.Lgs. n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.Lgs. 101/2018;

- Il D. Lgs. 10 marzo 2023, n. 24 Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del

Consiglio, del 23 ottobre 2019, riguardante 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.

Standard applicabili:

- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"

- ISO27017 controlli di sicurezza sulle informazioni

- ISO27018 per la protezione dei dati personali nei servizi Public Cloud

- Qualifica AGID

- Certificazione CSA Star

CONTESTO

Dati, processi e risorse di supporto

Tipologia dei dati trattati

I dati trattati sono quelli che riguardano le procedure di segnalazione di cui al d. lgs. n. 24 del 2023: l'identità del segnalante, il contenuto della segnalazione di violazione di norme di legge anche eurounitarie e l'identità del soggetto a cui la segnalazione si riferisce. In virtù del Contratto di servizio il Fornitore esegue operazioni di trattamento di dati personali (di seguito, "Dati Personali") di titolarità del Committente, e riferiti unicamente ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare l'acquisizione e l'archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

Il ciclo di vita del trattamento dei dati

I dati trattati sono quelli che riguardano le procedure di segnalazione di cui al d. lgs. n. 24 del 2023: l'identità del segnalante, il contenuto della segnalazione di violazione di norme di legge anche eurounitarie e l'identità del soggetto a cui la segnalazione si riferisce. In virtù del Contratto di servizio il Fornitore esegue operazioni di trattamento di dati personali (di seguito, "Dati Personali") di titolarità del Committente, e riferiti unicamente ai dati necessari per l'erogazione dei servizi pattuiti tra le parti. In particolare l'acquisizione e l'archiviazione delle segnalazioni dà luogo a trattamenti di dati personali appartenenti anche a particolari categorie di dati e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati, riferiti agli interessati, ovvero alle persone fisiche (identificate o identificabili) che inoltrano una segnalazione o a quelle indicate come possibili responsabili delle condotte illecite o a quelle a vario titolo coinvolte nelle vicende segnalate (art. 4, par. 1, nn. 1) e 2), del Regolamento.

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.

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. Cancellazione della piattaforma 15 giorni dopo la disattivazione del servizio.

Le risorse di supporto ai dati

Il Sistema di WhistelblowingPA si avvale di un 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).

PRINCIPI FONDAMENTALI

Proporzionalità e necessità

Gli scopi del trattamento dei dati

Gli scopi del trattamento sono specifici, espliciti e legittimi, in quanto i dati personali sono raccolti e trattati dal Comune di Gabbioneta Binanuova esclusivamente per consentire agli interessati di effettuare le segnalazioni previste dal d. lgs n. 24 del 2023 (c.d. normativa sul whistleblowing).

Le basi legali che rendono lecito il trattamento

Il trattamento è lecito, ai sensi dell'art. 6, lett. a) del GDPR, in quanto l'interessato effettuando la segnalazione esprime implicitamente il proprio consenso al trattamento dei propri dati personali

Il trattamento è lecito, ai sensi dell'art. 6, lett. c) del GDPR, in quanto il Titolare del trattamento deve effettuarlo per adempiere agli obblighi legali previsti dal diritto dell'Unione (direttiva europea 2019/1937) e dal diritto dello Stato italiano (d. lgs. 24 del 2023)

Il trattamento è lecito, ai sensi dell'art. 6, lett. e) del GDPR, in quanto il trattamento è necessario per l'esecuzione dei compiti di interesse pubblico legati alla normativa anticorruzione di cui è investito il Titolare.

Adeguatezza, pertinenza e limiti: la minimizzazione dei dati

In applicazione del principio della pertinenza, le segnalazioni raccolte e l'identità del segnalante vengono raccolti in base a quanto rappresentato dal whistleblower. 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.

Esattezza ed 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

La policy di *data retention* di *default* delle segnalazioni è di 12 mesi, prorogabili al doppio sulle singole segnalazioni per scelta precisa del soggetto ricevente, con cancellazione automatica sicura delle segnalazioni scadute.

Il sistema prevede la cancellazione dell'intera piattaforma passati n. 15 giorni dalla disattivazione del servizio.

PRINCIPI FONDAMENTALI

Misure a tutela dei diritti degli interessati

L'informativa agli interessati

Gli interessati al trattamento sono informati tramite un'informativa liberamente consultabile sia sull'Amministrazione Trasparente del Comune che sul sito internet del Responsabile esterno (https://www.whistleblowing.it/assistenza/).

Modalità di ottenimento del consenso

Dato atto che per consenso dell'interessato si intende qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento; è lo stesso interessato effettuando la segnalazione ad esprimere implicitamente il proprio consenso al trattamento dei propri dati personali.

Esercizio del diritto di accesso e portabilità dei dati

Coloro che effettuano la segnalazione hanno diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati personali e altre informazioni specificate nell'art. 15 del GDPR.

Ai sensi dell'art. 20 del GDPR gli interessati hanno il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che li riguardano forniti a un titolare del trattamento e hanno il diritto di trasmettere tali dati a un altro titolare del trattamento senza impedimenti da parte del titolare del trattamento.

A tal fine possono utilizzare i seguenti recapiti pec: comune.gabbioneta-binanuova@pec.regione.lombardia.it – mail: segretario@comune.gabbionetabinanuova.cr.it.

Esercizio dei diritti di rettifica e cancellazione

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi di cui all'art. 17 GDPR.

A tal fine si possono utilizzare i seguenti recapiti pec: comune.gabbioneta-binanuova@pec.regione.lombardia.it – mail: segretario@comune.gabbionetabinanuova.cr.it.

Esercizio dei diritti di limitazione e opposizione

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento quando ricorre una delle ipotesi di cui all'art. 18 del GDPR e può opporsi al trattamento in essere nel rispetto dell'art. 21 del GDPR.

A tal fine si possono utilizzare i seguenti recapiti pec: comune.gabbioneta-binanuova@pec.regione.lombardia.it – mail: segretario@comune.gabbionetabinanuova.cr.it.

Responsabili esterni del trattamento e trasferimento dati al di fuori dell'UE

Gli obblighi del Responsabile esterno sono definiti tramite contratto sottoscritto dal legale rappresentante dell'Ente. Tali obblighi riguardano, oltre la Whistleblowing Solutions in qualità di Responsabile del trattamento, i seguenti soggetti: Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions e Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions).

RISCHI

Misure di prevenzione esistenti o pianificate

1) 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.

2) 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.

3) 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. 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.

4) 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.

5) Controlli sulle vulnerabilità

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 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.

6) Backup

I sistemi sono soggetti a backup remoto giornaliero con policy di data retention di 7 giorni necessari per finalità di disaster recovery.

7) 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.

8) 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.

9) 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.

10) Gestione incidenti di sicurezza e violazioni dei dati personali

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

11) 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.

12) Minimizzazione dei dati e anonimato

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.

RISCHI MAPPATI

a) ACCESSO ILLEGITTIMO AI DATI

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

Azioni ritorsive nei confronti del segnalante e pregiudizio alla sua reputazione.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

accesso non autorizzato ai sistemi del Comune per operazioni non consentite/non autorizzate, azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Controllo degli accessi logici, Sicurezza dell'hardware, Minimizzazione dei dati e anonimato, Controlli sulle vulnerabilità.

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

Limitata, le misure individuate, pianificate ed adottate contribuiscono a mitigare la gravità dei rischi individuati.

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

Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

RISCHI MAPPATI

b) MODIFICHE INDESIDERATE DEI DATI

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

Azioni ritorsive nei confronti del segnalante, impossibilità di portare a compimento la procedura di segnalazione volta ad impedire fenomeni di *mala gestio* della cosa pubblica.

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

Azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio.

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

Archiviazione, Backup, Controllo degli accessi logici, Tracciabilità, Lotta contro il malware, Sicurezza dell'hardware, Sicurezza dei canali informatici, Vulnerabilità, Crittografia, Manutenzione, Gestire gli incidenti di sicurezza e le violazioni dei dati personali.

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

Limitata, le misure individuate, pianificate ed adottate contribuiscono a mitigare la gravità dei rischi individuati.

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

Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

RISCHI MAPPATI

c) PERDITA DI DATI

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

Impossibilità di portare a compimento la procedura di segnalazione volta ad impedire fenomeni di *mala gestio* della cosa pubblica.

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

Accesso non autorizzato ai sistemi del Comune per operazioni non consentite/non autorizzate, azione di virus informatici o di programmi suscettibili di recare danno, spamming o tecniche di sabotaggio, furto o distruzione degli hardware.

Quali sono le fonti di rischio?

Un dipendente malintenzionato che usa la sua vicinanza al sistema e le sue competenze, una terza parte autorizzata che sfrutta i privilegi di accesso per accedere illegittimamente alle informazioni. Le motivazioni possono essere molteplici: dallo scherzo alla molestia, fino al dolo, alla vendetta, allo spionaggio, alla speranza di lucro, all'acquisizione di dati per fini di ulteriore sfruttamento, una terza parte malintenzionata o ignara che sfrutta la sua vicinanza fisica per accedere fraudolentemente al servizio, incidente o un sinistro verificatosi presso uno dei soggetti preposti al trattamento.

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

Manutenzione, Archiviazione, Backup, Controllo degli accessi logici, Sicurezza dell'hardware, Gestione degli incidenti di sicurezza e delle violazioni dei dati personali.

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

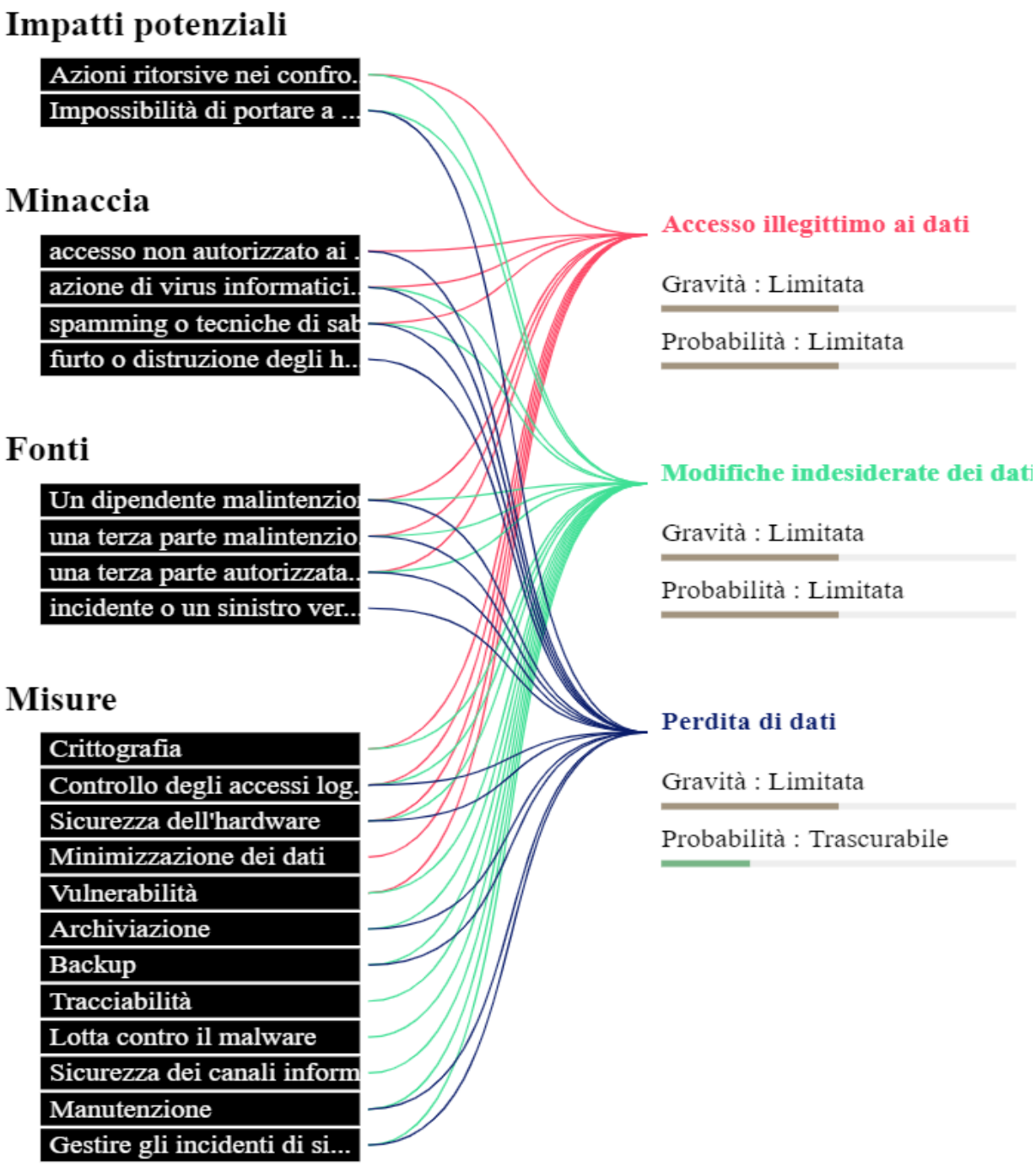
Limitata, le misure individuate, pianificate ed adottate contribuiscono a ridurre la gravità i rischi individuati

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

Trascurabile, le misure individuate, pianificate ed adottate contribuiscono a ridurre la probabilità che si verifichino i rischi individuati.

RISCHI

Panoramica dei rischi



Il titolare del trattamento
Il Sindaco
Antonio Bonazzoli

VALIDAZIONE

Nome del DPO

Avv. Alessia Roberto

Parere del DPO/RPD

Il trattamento appare adeguato. Il Titolare del Trattamento ha previsto una nuova soluzione organizzativa che prevede l'uso di nuove tecnologie che, 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 ha correttamente effettuato la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. La valutazione d'impatto è sufficientemente strutturata, e dà conto dei probabili rischi, che sono valutati ed adeguatamente mitigati dalle soluzioni adottate. In particolare, A seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati, a seguito dell'adozione delle misure di mitigazione del rischio indicate dall'ente, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto. Il sistema nel suo complesso coniuga in un ragionevole equilibrio il diritto alla riservatezza e protezione dei dati personali dei soggetti interessati con le attività di gestione dei trattamenti connessi allo 'whistleblowing', come da disposizioni normative.

Pertanto nel complesso, alla data odierna, non si ritiene esistente un "rischio elevato" come inteso dall'art. 35 GDPR; per tale ragione, inoltre, non si rende necessario procedere con la Consultazione preventiva ex art. 36 GDPR.

Richiesta del parere degli interessati

Non è stato chiesto il parere di interessati esterni perché non si sono individuate tali figure in modo chiaro e preciso perché la predisposizione del canale interno per le segnalazioni è un obbligo di legge (d. lgs. n. 24 del 2023) a cui la PA non può sottrarsi.

Gabbioneta Binanuova (CR), il __/__/2023

DPO

del Comune di Gabbioneta Binanuova

Avv. Alessia Roberto

_____