DPIA – Data Protection Impact Assessment

relativa al servizio di Whistleblowing Digitale basato su software GlobaLeaks ed erogato in modalità Software as a Service SaaS da Whistleblowing Solutions I.S. S.r.l.

Forno Canavese, 9 dicembre 2024

DPIA – DATA PROTECTION IMPACT ASSESSMENT 1
CONTESTO 4
Panoramica del trattamento 4
Responsabilità connesse al trattamento 4
Standard applicabili al trattamento 4
Prima valutazione 4
Dati, processi e risorse di supporto 4
Ciclo di vita del trattamento dei dati 5
Risorse di supporto ai dati 5
Seconda valutazione 5
PRINCIPI FONDAMENTALI 5
Proporzionalità e necessità 5
Terza valutazione 6
Basi giuridiche che rendono lecito il trattamento 6
Quarta valutazione 6
Adeguatezza, pertinenza e limitazione a quanto necessario in relazione alle finalità 6
Quinta valutazione 6
Esattezza e aggiornamento dei dati 6
Sesta valutazione 6
Periodo di conservazione dei dati 6
Settima valutazione 7
Misure a tutela dei diritti degli interessati 7
Ottava valutazione 7
Consenso degli interessati 7
Nona valutazione 7
ESERCIZIO DEI DIRITTI 7
Diritto di accesso e di portabilità dei dati 7
Diritti di rettifica e di cancellazione 7
Diritti di limitazione e di opposizione 8
Obblighi dei responsabili del trattamento 8
Trasferimento di dati extra UE 8
Decima valutazione 8
RISCHI 9
Crittografia 9
Undicesima valutazione 9
Anonimizzazione 9
Dodicesima valutazione 9
Controllo degli accessi logici 9
Tredicesima valutazione 10
Tracciabilità 10
Quattordicesima valutazione 10
Archiviazione 10
Quindicesima valutazione 10
Minimizzazione dei dati 10
Sedicesima valutazione 10
Vulnerabilità 10
Diciassettesima valutazione 10
Lotta contro il malware 11
Diciottesima valutazione 11
Sicurezza dei siti web 11
Diciannovesima valutazione 11
Contratto con il responsabile del trattamento 11
Ventesima valutazione 11
Politica di tutela della privacy 11
Ventunesima valutazione 11

INTEGRAZIONE DELLA PROTEZIONE DELLA PRIVACY NEI PROGETTI 11
VENTIDUESIMA VALUTAZIONE 12
GESTIONE DEGLI INCIDENTI DI SICUREZZA E DELLE VIOLAZIONI 12
VENTITREESIMA VALUTAZIONE 12
SICUREZZA DEI CANALI INFORMATICI 12
VENTIQUATTRESIMA VALUTAZIONE 12
GESTIONE DEL PERSONALE 12
VENTICINQUESIMA VALUTAZIONE 12
PRINCIPALI IMPATTI SUGLI INTERESSATI 12
VENTISEIESIMA VALUTAZIONE 13

Contesto

Panoramica del trattamento

Il trattamento per il quale si esegue la Valutazione di Impatto è la gestione delle segnalazioni di violazioni di disposizioni normative nazionali o dell'Unione europea che ledono l'interesse pubblico o l'integrità dell'amministrazione pubblica o dell'ente privato, di cui siano venute a conoscenza in un contesto lavorativo pubblico o privato, secondo quanto previsto dal DECRETO LEGISLATIVO 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).
In alcuni casi la piattaforma GlobaLeaks potrebbe essere utilizzata, attraverso differente canale e su richiesta del cliente titolare, per la gestione di comunicazioni interne aziendali per differenti finalità di compliance (diversity, SA8000, etc...).

Responsabilità connesse al trattamento

Whistleblowing Solutions I.S. S.r.l. ha il ruolo di Responsabile del trattamento dei dati personali relativi alle segnalazioni e comunicazioni.
Seeweb interviene in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions.
Transparency International Italia interviene in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions.
Il Comune di Forno Canavese riveste il ruolo di Titolare del trattamento.

Standard applicabili al trattamento

Attualmente, le Linee Guida ANAC "*Linee guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e protezione delle persone che segnalano violazioni delle disposizioni normative nazionali. Procedure per la presentazione e gestione delle segnalazioni esterne",* approvate con Delibera n°311 del 12 luglio 2023*)*) e Parere del Garante Privacy sulle stesse, oltre che i provvedimenti emessi dal Garante in materia di whistleblowing.

Prima valutazione

Accettabile

Dati, processi e risorse di supporto

Vengono trattati i dati forniti dal segnalante al fine di rappresentare le presunte condotte illecite delle quali sia venuto a conoscenza, trattati allo scopo di effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e l'adozione dei conseguenti provvedimenti. Vengono altresì trattati eventuali dati personali presenti nella documentazione allegata dal segnalante o da altri soggetti coinvolti. Infine, vengono trattate le informazioni di accesso e gli altri log relativi alle attività di admin e riceventi, eccezion fatta per il segnalante la cui attività non viene in alcun modo tracciata.
Le categorie di interessati sono: segnalanti, tutelati dalla normativa applicabile (a titolo esemplificativo, lavoratori subordinati, tirocinanti, consulenti del Titolare), nonché interessati che potrebbero essere menzionati dal segnalante o che potrebbero essere destinatari di ritorsioni in

ragione del ruolo assunto nel processo di segnalazione e/o del rapporto col segnalante (facilitatori, colleghi di lavoro etc…).
Inoltre, in caso di utilizzo della piattaforma per finalità di compliance diverse, potrebbero essere trattate con più probabilità categorie particolari di dati personali, relativi a differenti interessati, dunque non più strettamente limitati ai segnalanti così come definiti dalla normativa sul whistleblowing).

Ciclo di vita del trattamento dei dati

I dati di configurazione vengono inseriti da parte di utenti formalmente incaricati dal Titolare e, se presente, tramite documentazione allegata. I dati vengono conservati per il tempo necessario alla esecuzione delle finalità, come la gestione della segnalazione e apertura di istruttoria o archiviazione, e di ogni eventuale obbligo di legge, incluse le tempistiche previste per la conservazione dei log, nel rispetto delle prescrizioni di scadenza e cancellazione delle segnalazioni scelte dal Titolare. Allo scadere del periodo di conservazione, i dati relativi alla segnalazione vengono cancellati in maniera irreversibile dalla piattaforma.
Il Titolare ha comunque la possibilità di conservare i dati delle segnalazioni in un altro archivio, segregato.

Risorse di supporto ai dati

Come già detto, la piattaforma utilizzata è quella del provider GlobaLeaks. Pertanto, il servizio offerto da Whistleblowing Solutions I.S. S.r.l. trae naturale vantaggio dall'approccio e dalle funzionalità proprie di GlobalLeaks. A tale proposito, si osserva che nessun meccanismo o funzione di security viene disabilitato o indebolito in fase operativa, deployment incluso.
Le policy di configurazione rilevanti sono condivise con il cliente, con la proposizione di default sicuri e collaudati.
Nel contesto del trattamento effettuato dal Titolare, il Responsabile del trattamento acquisisce e mantiene i log relativi alle attività, accessi e operazioni, effettuate unicamente dagli amministratori di sistema e dagli altri soggetti autorizzati al trattamento, inclusi gli addetti incaricati che gestiscono le utenze del sistema e attribuiscono loro i relativi profili di autorizzazione). Al contrario, non vengono mai tracciati log e dati relativi alle connessioni alla piattaforma effettuate dal segnalante.
La piattaforma adotta uno schema di cifratura *in-use,* che prevede la persistenza nella piattaforma di soli dati cifrati, siano essi relativi alle segnalazioni immessi dal segnalante o riguardanti qualsiasi tipo di comunicazione ad esse relativa, come commenti, allegati, metadati collegati, ecc. L'utilizzo della piattaforma non contempla la possibilità che i dati siano trattati o salvati su supporti cartacei: la modalità del trattamento è interamente elettronica.

Seconda valutazione

Accettabile

Principi Fondamentali

Proporzionalità e necessità

Le finalità sono specifiche e legittime in quanto previste dalla normativa applicabile sia in ambito europeo che in ambito nazionale. In merito a tale trattamento si è già espresso il Garante Privacy con parere sulle Linee Guida ANAC in materia di whistlebowing.

Inoltre, per le ulteriori finalità di compliance diverse dal whistleblowing (SA8000, diversity etc...), tali finalità sono previste da altrettanti standard normativi.
La finalità dell'organizzazione in qualità di Responsabile è l'esecuzione del contratto e l'erogazione del servizio verso il cliente Titolare del trattamento.

Terza valutazione
Accettabile

Basi giuridiche che rendono lecito il trattamento
il trattamento effettuato dal Titolare del trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare (art..6. par. 1, lett. c), 9, par. 2, lett. b), e 10 del GDPR) nonchè per l'esecuzione di un compito di interesse pubblico contemplato dall'ordinamento (artt. 6 par. 1, lett e), e 9 par. 2, lett g) del GDPR).
Whistleblowing Solutions I.S. S.r.l. tratterà i dati del titolare in qualità di provider responsabile del trattamento per la esecuzione del contratto firmato tra le parti

Quarta valutazione
Accettabile

Adeguatezza, pertinenza e limitazione a quanto necessario in relazione alle finalità
I dati trattati sono quelli volontariamente inseriti da parte del segnalante o dagli altri utenti autorizzati dal Titolare, a seconda della loro funzione e ruolo nell'uso della piattaforma. Vengono poi tracciati i log e le informazioni di accesso e utilizzo della piattaforma da parte degli admin e degli altri utenti (eccetto il segnalante) per le finalità previste dalla normativa stessa.

Quinta valutazione
Accettabile

Esattezza e aggiornamento dei dati
La qualità dei dati viene garantita dal Titolare del trattamento attraverso l'operato dei soggetti autorizzati alla gestione delle segnalazioni secondo quanto previsto dal "modello organizzativo" proposto da Whistleblowing Solutions I.S. S.r.l.

Sesta valutazione
Accettabile

Periodo di conservazione dei dati
La data retention è stata determinata dal Titolare.
Di default, GlobaLeaks propone di default una *standard report retention policy*, trascorsa la quale la segnalazione scade e viene cancellata, di 180 giorni. Questa policy è frutto di una corretta valutazione tra benefici e costi, sia operativi che di privacy. Tale policy è tuttavia modificabile a cura del Titolare del trattamento che può estendere il periodo di conservazione fino ai 5 anni prescritti dalla norma.

Settima valutazione
Accettabile

Misure a tutela dei diritti degli interessati
Una prima e fondamentale misura di tutela è data attraverso l'informativa privacy che il Titolare del trattamento ha inserito all'interno della piattaforma e nel sito internet del Comune, secondo le modalità previste e decise dal Titolare del trattamento.

Ottava valutazione
Accettabile

Consenso degli interessati
Ove applicabile, il Titola del trattamento può utilizzare un apposito flag di raccolta del consegno, in abbinamento con la corrispondente informativa privacy.

Nona valutazione
Accettabile

Esercizio dei diritti

Diritto di accesso e di portabilità dei dati
La normativa di protezione dei dati prevede una specifica disposizione a tutela della riservatezza dell'identità del segnalante (d.lgs. 10 agosto 2018, n. 10121 di recepimento del Regolamento (UE) n. 2016/679, l'art. 2-undecies nel d.lgs. 30 giugno 2003, n. 196), che stabilisce che nell'ambito di una segnalazione whistleblowing, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) n. 2016/679, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante. In tal caso, dunque, al soggetto segnalato è preclusa la possibilità di rivolgersi al titolare del trattamento e, nel caso la facesse, in ovvia assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della Privacy (ai sensi dell'art. 77 dal Regolamento (UE) n. 2016/679). Resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di esercitare i propri diritti con le modalità previste dall'art. 160 d.lgs. n. 196/2003, e cioè di richiedere i diritti in questione per il tramite del Garante. Il Garante informa l'interessato di avere eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. È altresì previsto che il Titolare del trattamento informi l'interessato di tale facoltà.

Diritti di rettifica e di cancellazione
La normativa di protezione dei dati prevede una specifica disposizione a tutela della riservatezza dell'identità del segnalante (d.lgs. 10 agosto 2018, n. 10121 di recepimento del Regolamento (UE) n. 2016/679, l'art. 2-undecies nel d.lgs. 30 giugno 2003, n. 196), che stabilisce che nell'ambito di

una segnalazione whistleblowing, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) n. 2016/679, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante. In tal caso, dunque, al soggetto segnalato è preclusa la possibilità di rivolgersi al titolare del trattamento e, nel csso lo facesse, in ovvia assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della Privacy (ai sensi dell'art. 77 dal Regolamento (UE) n. 2016/679). Resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di esercitare i propri diritti con le modalità previste dall'art. 160 d.lgs. n. 196/2003, e cioè di richiedere i diritti in questione per il tramite del Garante. Il Garante informa l'interessato di avere eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. È altresì previsto che il Titolare del trattamento informi l'interessato di tale facoltà.

Diritti di limitazione e di opposizione

La normativa di protezione dei dati prevede una specifica disposizione a tutela della riservatezza dell'identità del segnalante (d.lgs. 10 agosto 2018, n. 10121 di recepimento del Regolamento (UE) n. 2016/679, l'art. 2-undecies nel d.lgs. 30 giugno 2003, n. 196), che stabilisce che nell'ambito di una segnalazione whistleblowing, il soggetto segnalato, presunto autore dell'illecito, con riferimento ai propri dati personali trattati, non può esercitare i diritti previsti dagli articoli da 15 a 22 del Regolamento (UE) n. 2016/679, poiché dall'esercizio di tali diritti potrebbe derivare un pregiudizio alla tutela della riservatezza dell'identità del segnalante. In tal caso, dunque, al soggetto segnalato è preclusa la possibilità di rivolgersi al titolare del trattamento e, nel csso lo facesse, in ovvia assenza di risposta da parte di quest'ultimo, di proporre reclamo al Garante della Privacy (ai sensi dell'art. 77 dal Regolamento (UE) n. 2016/679). Resta ferma la possibilità per il soggetto segnalato, presunto autore dell'illecito, di esercitare i propri diritti con le modalità previste dall'art. 160 d.lgs. n. 196/2003, e cioè di richiedere i diritti in questione per il tramite del Garante. Il Garante informa l'interessato di avere eseguito tutte le verifiche necessarie o di aver svolto un riesame, nonché del diritto dell'interessato di proporre ricorso giurisdizionale. È altresì previsto che il Titolare del trattamento informi l'interessato di tale facoltà.

Obblighi dei responsabili del trattamento

Il Titolare del trattamento ha provveduto a nominare Whistleblowing Solutions I.S. S.r.l. in qualità di responsabile del trattamento. Whistleblowing Solutions I.S. S.r.l. ha provveduto a nominare i sub-responsabili del trattamento coinvolti nell'erogazione del servizio: Seeweb per la gestione della piattaforma e dell'archiviazione hosting cloud IasS; Transparency International Italia per il supporto agli utenti e per l'assunzione del ruolo di amministratore di sistema.
Whistleblowing Solutions I.S. S.r.l. propone un proprio standard di nomina correlato al contratto di servizio.

Trasferimento di dati extra UE

I dati trattati vengono conservati in territorio Europeo.

Decima valutazione

Accettabile

Rischi

Crittografia

La piattaforma implementa uno schema di cifratura in-use, oggetto di security assessment specifico da parte del fornitore, che prevede la persistenza esclusivamente cifrata, sul DB, delle segnalazioni e di ogni comunicazione ad essi relativa. Lo schema prevede l'utilizzo di chiavi per-user e per-report, con il ricorso a meccanismi di Key Recovery e, opzionalmente, di Key Escrow per consentire un adeguato bilanciamento di security-usability.

Undicesima valutazione

Accettabile

Anonimizzazione

Il questionario prevede la possibilità per il segnalante di dichiarare la propria identità o di non dichiararla.
La piattaforma GlobaLeaks adotta un approccio rigoroso in relazione alla protezione dell'anonimato del segnalante.
La piattaforma tiene traccia delle attività effettuate da gli utenti, riceventi e admin, ma non di quelli relativi al segnalante.
I log eventi generati dallo stack applicativo di GlobaLeaks non contengono mai alcun IP address relativo al segnalante. Nella sezione "Audit log" della piattaforma vengono indicati soltanto gli eventi *whistleblower_login, whistleblower_logout, whistleblower_new_report,* con data e ora dell'evento ma senza alcun identificativo correlato (a differenza dei log relativi agli altri utenti).
Al riguardo la piattaforma dichiara quanto segue:
• "GlobaLeaks does not record IP address, information about the browser, the computer, or operating system of its users. Furthermore, the application does not embed any third-party content or deliver persistent cookies to your browser."
• "The application is offering the best anonymous technology now available such as Tor Onion Services and HTTPS with A+ grade certificates without any personal data retention."
• [Globaleaks] "does not leave traces in browser cache".

Dodicesima valutazione

Accettabile

Controllo degli accessi logici

Di default, così come previsto da GlobaLeaks, viene proposta un'autenticazione di livello "strong", a due fattori:
"Strong: A strong password should be formed by capital letters, lowercase letters, numbers and a symbols, be at least 12 characters long and include a variety of at least 10 different inputs."
The system enforces users to change their own password at their first login. Administrators could as well enforce password change for users at their next login.
The system identifies multiple failed login attempts and implement a slowdown procedure where an authenticating client should wait up to 42 seconds to complete an authentication.

This feature is intended to slow down possible attacks requiring more resources to users in terms of time, computation and memory.
Gli amministratori sono autenticati con 2FA e OTP.
La piattaforma tiene traccia delle attività effettuate da tutti gli utenti, riceventi e admin, ma non di quelli relativi al segnalante.
I log eventi generati dello stack applicativo di GlobaLeaks non contengono mai alcun IP address relativo a segnalanti. Nella sezione Audit log vengono indicati soltanto gli eventi *whistleblower_login, whistleblower_logout, whistleblower_new_report,* con data e ora dell'evento ma senza alcun identificativo correlato (a differenza dei log relativi agli altri utenti).

Tredicesima valutazione
Accettabile

Tracciabilità
Nel contesto del trattamento effettuato dal Titolare del trattamento, vengono acquisiti e mantenuti log relativi alle attività (accessi e operazioni) effettuate dal Responsabile del trattamento e dagli altri soggetti autorizzati al trattamento, non quelle effettuate dal segnalante.
I log sono visibili agli amministratori all'interno della sezione Audit log che raccogli i dettagli dei log come data, utente, tipo di log (login, logout, access_report per la stampa, delete_report in caso di cancellazione).

Quattordicesima valutazione
Accettabile

Archiviazione
La retention della segnalazione è impostata di default a 180 giorni, salvo diversa richiesta.

Quindicesima valutazione
Accettabile

Minimizzazione dei dati
La minimizzazione dei dati viene applicata by design raccogliendo i dati strettamente necessari alla corretta erogazione del servizio, ivi compresa la possibilità per il segnalante di indicare la propria identità o compilare il questionario in modo anonimo.

Sedicesima valutazione
Accettabile

Vulnerabilità
È stato visto e valutato il report AVA pubblicato dal fornitore GlobaLeaks (agosto 2022). Inoltre, è stata implementata la ricezione di notifiche per aggiornamenti software al fine di verificare se eventuali vulnerabilità sono state sanate in modo da adeguare gli aggiornamenti.

Diciassettesima valutazione
Accettabile

Lotta contro il malware

Il Responsabile del trattamento adotta strumenti anti-malware avanzati. La stessa cosa fa il Titolare del trattamento.
Per contro, non è disponibile all'interno della piattaforma uno strumento di scansione degli allegati inseriti dal segnalante o dal ricevente. La messa a disposizione di tale strumento implicherebbe infatti una gestione meno sicura dei documenti.

Diciottesima valutazione

Accettabile

Sicurezza dei siti web

La configurazione dei sistemi utilizzati dal Responsabile del trattamento per erogare il servizio prevede misure di hardening. Inoltre, sono implementate nel software della piattaforma GlobaLeaks le contromisure idonee a neutralizzare tutte le principali vulnerabilità OWASP.
È opportuno verificare che il Responsabile del trattamento abbia posto in essere misure di vulnerability assessment e gestione delle vulnerabilità sullo stack applicativo.

Diciannovesima valutazione

Accettabile

Contratto con il responsabile del trattamento

Il contratto di servizio proposto dal Responsabile del trattamento è chiaro ed esaustivo e non propone condizioni critiche o vessatorie.
I sub-responsabili del trattamento sono anch'essi contemplati nel contratto di servizio proposto da Whistleblowing Solutions I.S. S.r.l.

Ventesima valutazione

Accettabile

Politica di tutela della privacy

L'organizzazione ha una figura interna preposta a presidio delle tematiche privacy e protezione dei dati e un consulente esterno che riveste la figura di DPO.

Ventunesima valutazione

Accettabile

Integrazione della protezione della privacy nei progetti

La piattaforma GlobaLeaks è stata sviliuppata prendendo in considerazione il principio del privacy by design tramite strumenti di gestione delle attività (DevOps). Nello specifico, sono stati aperti task in merito ai "requisiti privacy e security" e alle specifiche tematiche di gestione dei dati, degli accessi e dei log, della retention delle segnalazioni, etc...

Ventiduesima valutazione
Accettabile

Gestione degli incidenti di sicurezza e delle violazioni
L'organizzazione ha adottato una procedura di gestione dei data breach che prevede uno specifico flusso per la comunicazione di una eventuale violazione dei dati all'Autorità Garante. La procedura prevede l'immediato coinvolgimento del Responsabile del trattamento per l'acquisizione delle informazioni necessarie e per l'adozione delle opportune misure di contenimento del danno e del DPO per la valutazione dell'impatto e dell'eventuale notifica al Garante.

Ventitreesima valutazione
Accettabile

Sicurezza dei canali informatici
Al fine di prevenire e rispondere ad attacchi cyber e garantire un adeguato livello di sicurezza, il Responsabile del trattamento ha implementato strumenti di monitoraggio ed analisi del traffico di rete e dei processi run-time sui server utilizzati per l'erogazione del servizio.

Ventiquattresima valutazione
Accettabile

Gestione del personale
Il trattamento dei dati personali viene effettuato soltanto da persone facenti parte della struttura del Titolare del trattamento, debitamente autorizzate al trattamento e impegnate al vincolo di riservatezza. Tali autorizzati al trattamento hanno ricevuto un'adeguata formazione in materia di protezione dei dati personali.

Venticinquesima valutazione
Accettabile

Principali impatti sugli interessati
Potrebbero verificarsi danni patrimoniali, danni non patrimoniali, danni alla riservatezza, danni morali.
Le principali minacce che potrebbero causare i sopra elencati impatti sono la sottrazione di credenziali di accesso, lo sfruttamento di vulnerabilità, l'attacco ai fornitori di servizi, l'attacco all'organizzazione del Comune.
Le principali fonti di rischio possono essere individuate nei dipendenti del Comune operanti in via accidentale o dolosa, nei virus e negli altri attacchi informatici, nei difetti software, nei dipendenti del Responsabile del trattamento o dei sub-responsabili del trattamento operanti in via accidentale o dolosa.
Le misure individuate per mitigare il rischio sono:

- il controllo degli accessi logici,

- la sicurezza dei siti web,
- la sicurezza dei canali informatici,
- la lotta contro il malware,
- la minimizzazione dei dati,
- la neutralizzazione delle vulnerabilità,
- l'anonimizzazione,
- l'uso di chiavi di Crittografia,
- l'integrazione della protezione della privacy nei progetti,
- la gestione del personale.

La valutazione della gravità del rischio, alla luce degli impatti potenziali e delle misure pianificate è indicata come "importante" considerate le categorie di dati personali che possono essere trattati, e dunque la varietà dei soggetti a rischio. I rischi, come si è visto, possono essere di vario tipo, da rischi di danni patrimoniali ed economici a rischi legati a danni psicologici o morali come: esposizione a ricatti, molestie, mobbing, discriminazione, licenziamento, mancato avanzamento di carriera.
La probabilità che uno o più di questi rischi possa cagionare un danno concreto agli interessati è però limitata grazie alle misure implementate. la probabilità dei rischi di cui sopra si riduce, anche in considerazione dell'affidabilità dei fornitori utilizzati.

Ventiseiesima valutazione

Accettabile

La presente Valutazione di Impatto (DPIA) è stata effettuata dal Dott. UMBERTO Bovenzi – Segretario Comunale e approvata dal Sindaco del Comune di Forno Canavese

(firma)

Parere del DPO sulla DPIA – Data Protection Impact Assessment

Il parere del DPO sulla DPIA – Data Protection Impact Assessment relativa al servizio di Whistleblowing Digitale basato su software GlobaLeaks ed erogato in modalità Software as a Service SaaS da Whistleblowing Solutions I.S. S.r.l. è il seguente:
"Il produttore e fornitore della piattaforma, GlobaLeaks ha adottato un insieme di misure di sicurezza molto robusto. Alle suddette misure di sicurezza sono state aggiunte da Whistleblowing Solutions I.S. S.r.l. ulteriori misure sia di riduzione della verosimiglianza (probabilità) del rischio che di mitigazione delle possibili conseguenze. Alcune scelte operate da Whistleblowing Solutions I.S. S.r.l. relativamente alla modalità di fruizione della piattaforma, alla trasparenza dell'interfaccia sia con i segnalanti che con i gestori delle segnalazioni, alla minimizzazione dei dati hanno ulteriormente contribuito alla riduzione della probabilità del rischio. La gravità del rischio resta potenzialmente alta, anche successivamente all'adozione delle misure di mitigazione che rientrano nella disponibilità di Whistleblowing Solutions I.S. S.r.l. Ulteriori misure di mitigazione, in particolare di riduzione del rischio e delle possibili conseguenze da atti di ritorsione, restano di competenza del Comune di Forno Canavese, Titolare di trattamento.
Pertanto, in virtù di quanto esposto, si ritiene che la limitata verosimiglianza del rischio legittimi l'effettuazione del trattamento."

Torino, 9 dicembre 2024

Il DPO
(Luciano Corino)