PROVINCIA DI PISA

DOCUMENTO DI VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI RELATIVI AL TRATTAMENTO NELL'AMBITO DELLA PROCEDURA DI WHISTLEBLOWING

(DPIA - *DATA PROTECTION IMPACT ASSESSMENT*)

Redatto ai sensi dell'articolo 35 del Regolamento UE 679/2016 e delle Linee Guida WP248 rev. 01 adottate il 4 Aprile 2017 in materia di valutazione d'impatto sulla protezione dei dati e determinazione delle possibilità che il trattamento "possa presentare un rischio elevato".

Titolare del trattamento:

Provincia di Pisa

Legale rappresentante:

Presidente della Provincia Dott. Massimiliano Angori

Responsabile della protezione dei dati (RPD/DPO):

Avv. Marco Giuri

Sede

Piazza Vittorio Emanuele II , n. 14, Pisa

Data

INTRODUZIONE

MOTIVAZIONE DELLA VALUTAZIONE

Il presente documento viene elaborato sulla scorta dell'articolo 35 del Regolamento UE 679/2016.

La valutazione d'impatto si rende necessaria alla luce di un'attenta autoanalisi compiuta circa il trattamento dei dati personali.

La Provincia di Pisa, quale Ente Pubblico, ritiene necessario procedere ad una valutazione di impatto, stante il rischio elevato che il ***trattamento di dati personali nell'ambito della procedura di whistleblowing*** può avere sui diritti e le libertà delle persone fisiche, in ragione delle caratteristiche di pervasività e possibile intrusione nella sfera dei comportamenti personali, proprie dello stesso .

L'art. 35 del GDPR prevede infatti che "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.

Inoltre, al par. 7 il legislatore europeo stabilisce: "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;

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".

La valutazione di impatto si riferisce alla valutazione dei rischi in cui potrebbero incorrere le libertà ed i diritti dei cittadini dall'utilizzo della piattaforma informatica gratuita individuata (Whistleblowing Solutions I.S. S.r.l.).

Il Titolare del trattamento provvederà: - all'adozione di politiche di controllo periodiche in riferimento ai dati oggetto del trattamento in questione e alle misure esistenti o pianificate (misure applicate ai dati, misure generali di sicurezza dei sistemi e misure organizzative); ad effettuare una

precisa e rigorosa manutenzione dei sistemi; alla costante formazione del personale designato/autorizzato al trattamento dei dati. La DPIA viene pubblicata sul sito web della Provincia di PISA, sezione Amministrazione Trasparente – Altri contenuti – Prevenzione della Corruzione - Whistleblowing

CONTESTO

PANORAMICA DEL TRATTAMENTO

Il trattamento oggetto della presente DPIA è relativo alla acquisizione e gestione delle **segnalazioni di illeciti c.d. whistleblowing** ai sensi del **d.lgs. 24 del 10 marzo 2023** che recepisce **la Direttiva UE 1937/2019.**

Responsabilità connesse al trattamento

Provincia di Pisa: titolare del trattamento nella persona del Presidente *pro tempore.*
RPCT dell'Ente: gestore del trattamento è l' RPCT dell'Ente.
WHISTLEBLOWING SOLUTION SRL: responsabile del trattamento
SEE WEB: sub-responsabile del trattamento nominato da whistleblowing solutions srl per la gestione dell'infrastruttura informatica (Iaas).
Transparency International Italia: Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing.

Standard applicabili al trattamento

D. LGS N.24 del 2023
Direttiva UE n.1937/2019
LL. GG. ANAC approvate con Delibera n. 311 del 12 Luglio 2023
LL.GG. ANAC approvate con Delibera n. 478 del 26 Novembre 2025

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

(vedi allegato 1)

DATI, PROCESSI E RISORSE DI SUPPORTO

Categorie di dati trattati

I dati trattati sono quelli inseriti nella segnalazione e nel caso, acquisiti nel corso della conseguente istruttoria. Tali dati possono essere sia dati comuni (identità del segnalante, del segnalato, i ruoli ricoperti dagli stessi), sia dati particolari e relativi a condanne penali e reati, eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.

Ciclo di vita del trattamento dei dati (descrizione funzionale)

Il trattamento dei dati oggetto della presente D.P.A. si articola nelle seguenti fasi:

Ricezione e Raccolta: Attivazione della piattaforma, invio della segnalazione, autenticazione e cifratura dei dati.

Gestione e Analisi: Accesso alla piattaforma limitato agli autorizzati, istruttoria, interlocuzione con il segnalante e indagini interne.

Chiusura e feedback: Comunicazione dell'esito della segnalazione al segnalante entro tre mesi dalla conferma di ricezione.

Conservazione e archiviazione: i dati non utili alla gestione non sono raccolti o, se raccolti accidentalmente, eliminati.

La documentazione è conservata per il tempo necessario (non oltre i 5 anni dall'esito finale). Nel caso di contenzioso o segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrebbe essere protratto anche oltre i termini sopraindicati, sino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.

Risorse di supporto ai dati

La Provincia di Pisa si avvale, per la gestione delle segnalazioni, di una piattaforma informatica di segnalazione basata su software libero e open-source Global leaks di cui Whistleblowing Solutions è coautore e coordinatore di progetto.
L' infrastruttura IaaS e SaaS privata è basata sulle seguenti tecnologie:
- Dettaglio Hardware
- VMWARE (virtualizzazione)
- Debian Linux LTS (sistema operativo)
- VEEAM (backup)
- OPNSENSE (firewall)
- OPENVPN (vpn).
(Vedi allegato1-Documento di supporto del responsabile del trattamento).

La gestione delle segnalazioni non avviene tramite altri canali. Infatti, anche nell'ipotesi in cui il segnalante chieda un appuntamento a RPCT, quest'ultimo provvederà a inserire la segnalazione raccolta oralmente direttamente nella piattaforma. Tutte le attività istruttorie, avviate in seguito alla segnalazione, sono gestite nell'ambito della piattaforma, così come le comunicazioni con il segnalante, il segnalato ed eventuali ulteriori soggetti (informatori).

PRINCIPI FONDAMENTALI

PROPORZIONALITÀ E NECESSITÀ

Finalità trattamento

Il trattamento è necessario per adempiere a un obbligo legale a cui è soggetto il titolare del trattamento ed è relativo alle procedure c.d. whistleblowing sono trattati esclusivamente per ricevere e gestire le segnalazioni di violazioni presentate ai sensi del D. Lgs. 10 marzo 2023, n. 24, effettuare le necessarie attività istruttorie volte a verificare la fondatezza del fatto oggetto di segnalazione e procedere all’adozione di tutti i conseguenti provvedimenti. I dati non sono trattati per ulteriori finalità.

Basi legali che rendono lecito il trattamento

Il trattamento di dati comuni (dati identificativi e di contatto del segnalante, dell'autore delle violazioni o di altre persone a vario titolo coinvolte nelle vicende segnalate) costituisce l'adempimento di un obbligo legale e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR. Nel caso in cui vengano trattati dati appartenenti a categorie particolari, la base giuridica è rappresentata dall'art. 9.2, lett. b) e g) GDPR, in connessione con l'art. 2-sexies, comma 2, lett. dd), del D.Lgs. n.196/2003. Per i dati personali relativi a condanne penali e misure di sicurezza, la base giuridica è rappresentata dall'art. 2-octies, comma 3, lett. a), del D.Lgs. n. 196/2003. I dati personali sono trattati sulla base del consenso espresso del segnalante ai fini della conoscibilità della segnalazione ove la stessa sia necessaria alla difesa dell'incolpato, anche nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023).

Adeguatezza, pertinenza e proporzionalità dei dati 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, 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.

Aggiornamento 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. Nel caso di segnalazioni palesemente infondate le stesse vengono immediatamente archiviate. Nel caso di informazioni non coerenti, nell'ambito dell'istruttoria RPCT e i soggetti autorizzati alla gestione della segnalazione possono aggiornare i dati, chiedere eventuali integrazioni o rettifiche che sono comunque inserite nel fascicolo della segnalazione. Inoltre, il segnalante può sempre interloquire con RPCT, tramite la piattaforma, al fine di chiedere la modifica / integrazione delle informazioni trasmesse.

Qual è il periodo di conservazione dei dati?

Le segnalazioni, e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque non oltre cinque anni, che decorrono dalla data di comunicazione dell'esito finale della procedura di segnalazione, come espressamente previsto dall'articolo 14 del D.lgs. n. 14/2023. Nel caso di contenzioso o di segnalazione all'Autorità giudiziaria, ad ANAC, il trattamento potrà essere protratto anche oltre i termini sopra indicati, fino al termine di decadenza di eventuali ricorsi e fino alla scadenza dei termini di prescrizione per l'esercizio dei diritti e/o per l'adempimento di altri obblighi di legge.
Specificatamente alla piattaforma informatica, come si legge all'allegato 1, sono previste:
-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.

MISURE A TUTELA DEI DIRITTI DEGLI INTERESSATI

Informativa privacy interessati

Gli interessati sono informati attraverso una specifica informativa resa ai sensi degli artt. 13-14 GDPR. L'informativa viene resa disponibile secondo le seguenti modalità:
• Comunicazione a tutti i dipendenti sull'esistenza del canale di segnalazione interno;
• Pubblicazione sito web istituzionale – sezione dedicata al Whistleblowing.

Consenso degli interessati

Il trattamento dei dati personali acquisiti con la segnalazione e nell'ambito delle successive attività istruttorie non necessita di consenso da parte dell'interessato, in quanto la base giuridica del trattamento è l'adempimento di un obbligo di legge e l'esecuzione di un compito di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e) del GDPR.
Il consenso degli interessati costituisce la base giuridica unicamente per la comunicazione dell'identità del segnalante al segnalato, ove la stessa sia necessaria alla difesa dell'incolpato nel procedimento disciplinare (art. 12, commi 2 e 5 del D.Lgs. n. 24/2023). La piattaforma consente di raccogliere il consenso del segnalante per tale fine al momento dell'invio della segnalazione, tramite apposito form.

Esercizio diritti di accesso e di portabilità dei dati

Quanto al diritto di accesso, si segnala che tale diritto non appare immediatamente esercitabile poiché limitato ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (...) f) alla riservatezza dell'identità della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993,

n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58". L'interessato può comunque avanzare la richiesta ai dati di contatto indicati dal Titolare del trattamento nell'informativa fornita ai sensi degli artt. 13 e 14 oppure contattando direttamente il Data Protection Officer nominato dall'Ente. La Provincia di Pisa effettuerà tutte le valutazioni del caso, tenendo sempre in considerazione l'obbligo di garantire la riservatezza del segnalante.

Esercizio diritti di rettifica e di cancellazione (diritto all'oblio)

Il diritto alla cancellazione non è applicabile al caso di specie, ai sensi dell'art. 17, par. 3, GDPR a norma del quale: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: (…) b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse".

Esercizio diritti di limitazione e di opposizione

Il diritto alla limitazione non appare esercitabile, ai sensi e per gli effetti dell'art. 2 undecies, co. 1, lett. f) D.lgs. 196/03 a norma del quale: "1. I diritti di cui agli articoli da 15 a 22 del Regolamento non possono essere esercitati con richiesta al titolare del trattamento ovvero con reclamo ai sensi dell'articolo 77 del Regolamento qualora dall'esercizio di tali diritti possa derivare un pregiudizio effettivo e concreto (...) f) alla riservatezza dell' identita' della persona che segnala violazioni di cui sia venuta a conoscenza in ragione del proprio rapporto di lavoro o delle funzioni svolte, ai sensi del decreto legislativo recante 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, ovvero che segnala violazioni ai sensi degli articoli 52-bis e 52-ter del decreto legislativo 1° settembre 1993, n. 385, o degli articoli 4-undecies e 4-duodecies del decreto legislativo 24 febbraio 1998, n. 58.

Non è previsto il riconoscimento del diritto di opposizione, sussistendo motivi legittimi cogenti per procedere al trattamento, in considerazione delle finalità di interesse pubblico perseguite, degli interessi connessi al buon andamento della PA, nonché della necessità e proporzionalità del trattamento medesimo.

Formalizzazione obblighi dei responsabili del trattamento

Whistleblowing PA Srl è stata formalmente nominata quale Responsabile del trattamento (All. 2). La Nomina risponde ai criteri di cui all'art. 28 GDPR.

Tutela dati in caso di trasferimento di dati al di fuori dell'Unione europea

Non è previsto alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

RISCHI

MISURE ESISTENTI O PIANIFICATE

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/stable/security/EncryptionProtocol.html

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.

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/stable/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 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.

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.

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.

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.

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.

Sicurezza dei documenti cartacei

La sicurezza dei documenti cartacei è garantita attraverso le seguenti misure:

- attività di trattamento dei dati riservata al solo personale autorizzato;
- accesso agli archivi e/o ad altro luogo in cui sono custoditi dati su supporto cartaceo al solo personale autorizzato;
- sensibilizzazione e formazione di tutto il personale dipendente, ivi compreso quello non autorizzato al trattamento dei dati personali;
- il trattamento dei dati (specie di quelli sensibili o particolari) deve avvenire solo all'interno dei locali protetti dell'Ente ed accessibili solo agli autorizzati;
- dotazione di sistemi di videosorveglianza;
- chiusura delle porte di accesso dei locali;
- guardiania portierata;
- chiusura a chiave degli archivi;
- armadi e contenitori dotati di serrature.

Il trattamento dei dati (specie di quelli sensibili o particolari) deve avvenire solo all'interno dei locali protetti dell'Ente ed accessibili solo agli autorizzati.

ACCESSO ILLEGITTIMO AI DATI

Principali impatti sugli interessati se il rischio si dovesse concretizzare

- Condotte ritorsive (il licenziamento, la sospensione o misure equivalenti, la retrocessione di grado o la mancata promozione, il mutamento di funzioni, il cambiamento del luogo di lavoro, la

riduzione dello stipendio, la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria, la coercizione, l'intimidazione, le molestie o l'ostracismo, la discriminazione o comunque il trattamento sfavorevole, la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione, il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche la perdita di redditi, l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro, la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso, la richiesta di sottoposizione ad accertamenti psichiatrici o medici).

- Conseguenze di carattere reputazionale
- Difficoltà nelle relazioni lavorative e sociali
- Aumento stress lavorativo
- Estorsione (anche sotto forme di tentativo) .
-

Principali minacce che potrebbero concretizzare il rischio

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco criptolocker che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;
- Spamming, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati. Il rischio de quo è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server,

che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione;

- Furto di credenziali di autentificazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;
- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati), o verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

Fonti di rischio

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente).

Fonti non umane: (acqua, materiali pericolosi, virus informatici generici).

Misure fra quelle individuate contribuiscono a mitigare il rischio

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

Gravità del rischio alla luce degli impatti potenziali e delle misure pianificate

Importante

Gli interessati potrebbero sperimentare conseguenze significative, anche irrimediabili, che potrebbero non superare.

In particolare condotte ritorsive (il licenziamento, la sospensione o misure equivalenti, la retrocessione di grado o la mancata promozione, il mutamento di funzioni, il cambiamento del luogo di lavoro, la riduzione dello stipendio, la modifica dell'orario di lavoro, la sospensione della formazione o qualsiasi restrizione dell'accesso alla stessa, le note di merito negative o le referenze negative, l'adozione di misure disciplinari o di altra sanzione, anche pecuniaria, la coercizione, l'intimidazione, le molestie o l'ostracismo, la discriminazione o comunque il trattamento sfavorevole, la mancata conversione di un contratto di lavoro a termine in un contratto di lavoro a tempo indeterminato, laddove il lavoratore avesse una legittima aspettativa a detta conversione, il mancato rinnovo o la risoluzione anticipata di un contratto di lavoro a termine; i danni, anche alla reputazione della persona, in particolare sui social media, o i pregiudizi economici o finanziari, comprese la perdita di opportunità economiche l'inserimento in elenchi impropri sulla base di un accordo settoriale o industriale formale o informale, che può comportare l'impossibilità per la persona di trovare un'occupazione nel settore o nell'industria in futuro, la conclusione anticipata o l'annullamento del contratto di fornitura di beni o servizi; l'annullamento di una licenza o di un permesso, la richiesta di sottoposizione ad accertamenti psichiatrici o medici).

Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Limitata

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte e come rappresentate nell'All. 1) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy. In particolare, le misure di sicurezza approntate proteggono la riservatezza dell'identità sia del whistleblower, sia della persona segnalata, sia di qualsiasi altra persona comunque menzionata nella segnalazione, nonché la riservatezza del contenuto della segnalazione e della relativa documentazione. Ciò è garantito anche tramite il ricorso a strumenti di crittografia.

MODIFICHE INDESIDERATE DEI DATI

Principali impatti sugli interessati se il rischio si dovesse concretizzare

Ingiusto coinvolgimento del segnalato in procedimenti disciplinari e/o giudiziari;, Condotte ritorsive di cui all' art. 12 d.lgs 24/2023

Principali minacce che potrebbero consentire la concretizzazione del rischio

- Negligente custodia delle credenziali di accesso alla Piattaforma;
- Utilizzo improprio / cessioni di credenziali per l'accesso alla Piattaforma;
- Intercettazioni delle trasmissione o dei dati;
- Data Breach subito dal Responsabili del trattamento;
- Violazione delle piattaforma da parte di attaccanti esterni.

Fonti di rischio

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente),
Fonti non umane: Possono essere un incidente o un sinistro verificatosi presso uno dei soggetti incaricati del trattamento (interruzioni di corrente, incendio, inondazione, ecc.

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

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

Gravità del rischio alla luce degli impatti potenziali e delle misure pianificate

Importante

La gravità del rischio è valutata importante in considerazione delle categorie dei soggetti interessati (soggetti segnalanti oggetto di possibili condotte ritorsive, ma anche soggetti segnalati passibili di procedimenti disciplinari o giudiziari a loro carico), nonché delle possibili conseguenze a carico degli stessi in caso di violazione dell'integrità dei dati.

Probabilità del rischio con riguardo a minacce, fonti di rischio e misure pianificate

Limitata

La probabilità di rischio è valutata limitata in quanto le attività di trattamento di cui la presente DPIA sono effettuate tramite l'utilizzo di piattaforma fornita da società che garantisce l'adeguatezza delle misure organizzative e di sicurezza (come sopra elencate e descritte) e la conformità delle stesse alle indicazioni di A.N.A.C. e del Garante Privacy.

PERDITA DI DATI

Impatti principali sugli interessati se il rischio dovesse concretizzarsi

Mancata definizione dell'istruttoria e conseguenti possibili problematiche di natura giuslavoristica e contrattuale.

Principali minacce che potrebbero consentire la materializzazione del rischio

- Data Breach subito dal Responsabili del trattamento;
- Violazione delle piattaforma da parte di attaccanti esterni;
- Furto di credenziali di autentificazione che potrebbe comportare un accesso non autorizzato alle banche dati, ai pc e agli archivi contenenti il trattamento dati in formato cartaceo;
- Perdita, diffusione e danneggiamento dei dati, e più in generale un trattamento illecito e non corrispondente alla finalità per cui i dati sono stati raccolti;
- Errore materiale nell'esecuzione dell'ufficio che potrebbe determinare il rischio di trattamenti illeciti, diffusioni, omissioni nel corretto e lecito trattamento;
- Errori umani nella gestione della struttura fisica (si pensi alla perdita e al danneggiamento dei dati per mancato inserimento del sistema di allarme, alla mancata revisione del sistema di antincendio o alla fortuita dimenticanza di aperture che facilitano l'ingresso di terzi non autorizzati);

- Attacco al sistema informatico da parte di virus, che potrebbe causare danneggiamento ai software e, per l'effetto, danneggiamento, perdita, alterazione e diffusione non autorizzata dei dati;
- Attacco criptolocker che potrebbe causare danneggiamento ai software e conseguente danneggiamento, perdita, diffusione non autorizzata dei dati;
- Spamming, che potrebbe determinare un danneggiamento ai software con conseguente alterazione, perdita, diffusione non autorizzata dei dati;
- Malfunzionamento per vetustà degli elaboratori e degli strumenti di lavoro;
- Accesso ai locali da parte di soggetti non autorizzati che potrebbero impossessarsi dei dati e dei dispositivi che li contengono, diffondendo illecitamente i dati;
- Accessi in rete non autorizzati;
- Il rischio de quo è anche ricollegabile agli interventi operati da parte dell'assistenza tecnica da remoto sulle macchine, sui software, sui computer e sui server, che potrebbero determinare, in modo del tutto inconsapevole, la cancellazione di dati, la loro diffusione e/o modificazione;
- Verificarsi di eventi distruttivi naturali o artificiali che possono causare la perdita e il danneggiamento delle macchine delle strutture e, conseguentemente, dei dati ivi conservati.

Fonti di rischio

Fonti non umane: es. acqua, materiali pericolosi, virus informatici generici);

Fonti umane: Persona, interna o esterna all'organismo o all'ente, operante in via accidentale o intenzionale (esempio: amministratore IT, utente, attaccante esterno, concorrente).

Quali misure contribuiscono a mitigare il rischio

Sicurezza dei canali informatici

Crittografia

Archiviazione

Tracciabilità

Vulnerabilità

Manutenzione

Backup

Lotta contro il malware

Sicurezza dell'hardware

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Controllo degli accessi logici

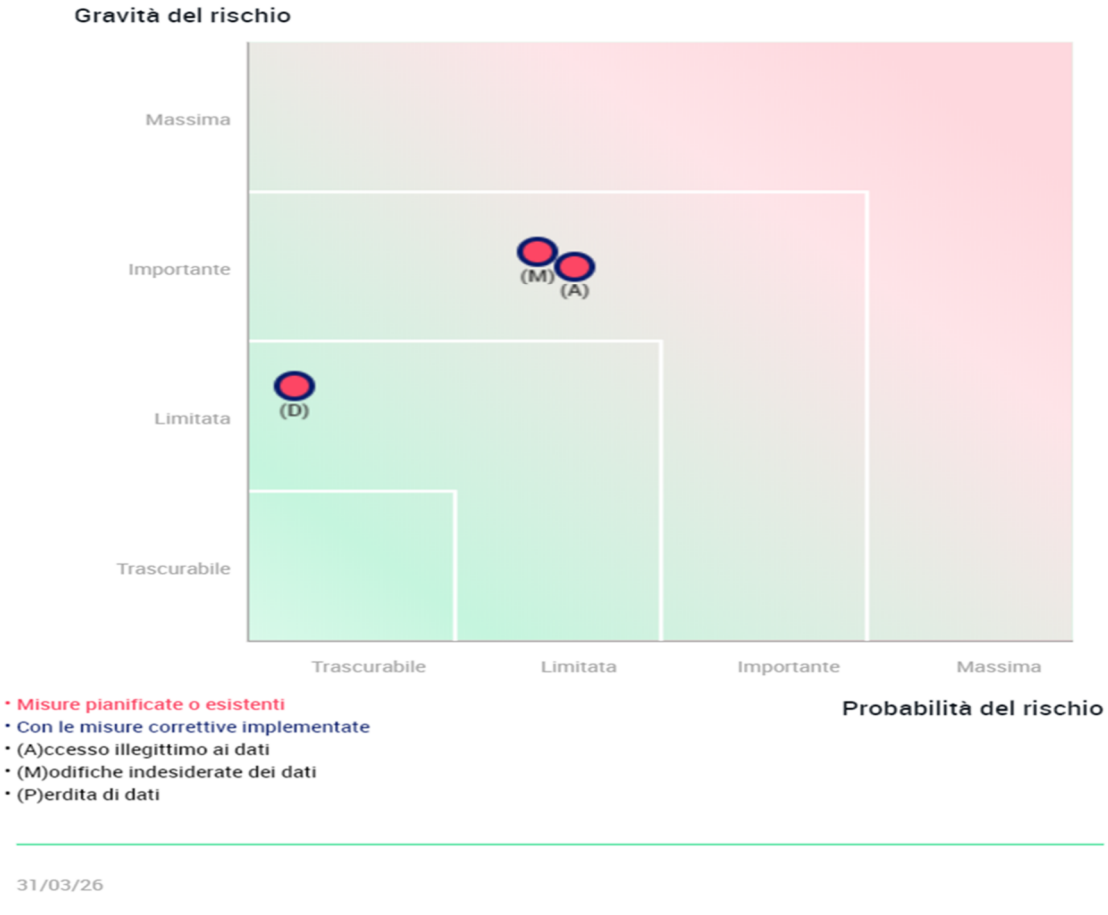
Sicurezza dei documenti cartacei

Gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate

Limitata, la perdita indesiderata dei dati potrebbe comportare ricadute nell'iter amministrativo dei processi dell'Ente, comportando possibili ricadute di natura contrattuale rispetto agli interessati. Tali difficoltà risultano comunque superabili anche se con spendita di tempo e di risorse dedicate alle necessarie rettifiche / integrazioni.

Probabilità del rischio con riguardo alle minacce, alle fonti di rischio e alle misure pianificate

Trascurabile, le politiche di gestione della vulnerabilità, nonchè i sistemi di backup adottati dal Responsabile del trattamento riducono la probabilità del rischio.



Ai sensi del paragrafo 2, art. 35 del GDPR si consulta il responsabile della protezione dei dati: questo viene sempre coinvolto nelle decisioni dell'Ente e viene richiesto il suo parere su singole questioni o quesiti che hanno a che fare con il trattamento dei dati personali.

Anche il presente documento verrà sottoposto al suo vaglio finale.

PARERE DEL DPO: POSITIVO rilasciato dall'Avvocato Marco Giuri in data 23 Aprile 2026.

CONCLUSIONI

Si ritiene che le contromisure adottate in vista di un rischio iniziale, determinato come alto, possano ragionevolmente abbassarlo ad un livello di sicura gestibilità da parte del Titolare.
In quest'ottica, si ritiene superflua, in accordo con il DPO, la consultazione preventiva dell'Autorità Garante, ai sensi e per gli effetti dell'art. 36 Regolamento UE 679/2016, in considerazione anche della disponibilità dell'Ente all'adozione di un graduale piano di adeguamento per assicurare la migliore sicurezza e protezione dei dati trattati da parte della Provincia.

Il Titolare del trattamento, in persona del Direttore Generale pro tempore, preso atto delle valutazioni sopra riportate in ordine all'analisi del potenziale impatto per i diritti e le libertà degli interessati, con l'adozione della presente DPIA, dispone che il documento sia reso pubblico sul sito internet istituzionale nell'apposita sezione WHISTLEBLOWING.

Il Direttore Generale/Segretario Generale

Dott. Danilo D'Aco

D' ACO
DANILO
15.07.2026
12:04:56
GMT+02:00