Comune di Arnesano

Valutazione d'impatto sulla protezione dei dati ai sensi del regolamento UE 2016/679, in relazione al trattamento di dati effettuato tramite la gestione delle segnalazioni di illeciti per contrastare i fenomeni corruttivi (WHISTLEBLOWING)

Sommario

Informazioni sulla DPIA

Nome della valutazione d'impatto

Valutazione di impatto in relazione al trattamento di dati effettuato tramite la gestione delle segnalazioni di illeciti per contrastare i fenomeni corruttivi e delle segnalazioni di illeciti nell'ambito dell'Ente locale.

Titolare del trattamento

Comune di Arnesano, in persona del Sindaco, Avv. Emanuele Solazzo

Nome autore

Segretario Generale, Dott. Pierluigi Cannazza

Nome valutatore

Avv. Marco Micella – Responsabile Protezione dei Dati

Nome validatore

Giunta comunale

Data
15/09/2023

Allegati:

- Nomina a responsabile del trattamento per Whistleblowing Solutions
- Sicurezza e Tecnologia (WBPA) di WhistleblowingPA

Nota di redazione: i commenti e le valutazioni del valutatore sono riportati nel documento all'interno di un campo colorato come il presente.
Il giudizio di valutazione dei singoli punti da parte del valutatore può essere:
Da correggere: l'analisi non è ritenuta accettabile e deve essere ripetuta.
Migliorabile: l'analisi è ritenuta accettabile a condizione che vengano svolti gli interventi migliorativi descritti
Accettabile: l'analisi è ritenuta accettabile senza prescrizioni

Contesto

Panoramica del trattamento

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati (Reg. UE 2016/679, c.d. GDPR), non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

La legge 6 novembre 2012, n.190 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione" ha introdotto, con l'articolo 1, comma 51, un nuovo articolo all'interno del D.Lgs. n. 165/2001 "Norme generali sull'ordinamento del lavoro alle dipendenze delle amministrazioni pubbliche", ovvero l'art. 54-bis (modificato, poi, dalla legge n.179/2017), rubricato "Tutela del dipendente pubblico che segnala illeciti".

Con determinazione n.6 del 28 aprile 2015, l'ANAC ha emanato apposite "*Linee guida in materia di tutela del dipendente pubblico che segnala illeciti*" (c.d. whistleblower) e, con delibera n.469 del 09 giugno 2021, l'ANAC ha emanato altresì nuove "*Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del D.lgs. 165/2001 (c.d. whistleblowing)*".

Il presente documento, pertanto, viene redatto al fine di effettuare una valutazione d'impatto sulla protezione dei dati, relativamente al trattamento finalizzato alla "gestione delle segnalazioni dipendenti e non (segnalazioni

relative a violazioni di legge, procedure, pericoli salute e sicurezza, conflitti di interesse, etc.) volte a prevenire i fenomeni corruttivi e altre attività criminose" - effettuato anche a seguito dell'introduzione degli obblighi derivanti dal D.Lgs. 10 marzo 2023 n. 24 - tramite specifica piattaforma web per la gestione delle segnalazioni di fenomeni corruttivi (WHISTLEBLOWING).

Ai fini della redazione del presente documento, si evidenzia che le condotte illecite oggetto di segnalazione non riguardano soltanto quelle che integrano le fattispecie penalmente rilevanti, ma anche quelle condotte:
i) poste in essere in violazione dei Codici di comportamento o di altre disposizioni sanzionabili in via disciplinare;
ii) suscettibili di arrecare un pregiudizio patrimoniale all'amministrazione di appartenenza o ad altro ente pubblico;
iii) suscettibili di arrecare un pregiudizio all'immagine dell'amministrazione;
iv) più in generale, situazioni in cui si riscontri l'abuso, da parte di un soggetto, del potere a lui affidato, al fine di ottenere vantaggi privati, nonché i fatti in cui, a prescindere dalla rilevanza penale, venga in evidenza un malfunzionamento dell'organizzazione, a causa dell'uso, a fini privati, delle funzioni attribuite.

Le caratteristiche delle modalità di segnalazione adottate dal Comune sono le seguenti:
• la segnalazione viene fatta attraverso la compilazione di un questionario e può essere inviata in forma anonima. Se anonima, sarà presa in carico solo se adeguatamente circostanziata;
• la segnalazione viene ricevuta dal Responsabile per la Prevenzione della Corruzione (RPC) e da lui gestita mantenendo il dovere di confidenzialità nei confronti del segnalante;
• nel momento dell'invio della segnalazione, il segnalante riceve un codice numerico di 16 cifre che deve conservare per poter accedere nuovamente alla segnalazione, verificare la risposta dell'RPC e dialogare rispondendo a richieste di chiarimenti o approfondimenti;
• la segnalazione può essere fatta da qualsiasi dispositivo digitale (pc, tablet, smartphone) sia dall'interno dell'ente che dal suo esterno. La tutela dell'anonimato è garantita in ogni circostanza.

Le segnalazioni possono essere inviate all'indirizzo web: https://comunediarnesano.whistleblowing.it/

Quale è il trattamento in considerazione?

Il trattamento preso in considerazione attiene al trattamento di dati effettuato tramite la gestione informatizzata delle segnalazioni di illeciti nell'ambito dell'Ente locale per contrastare i fenomeni corruttivi (nel campo delle attività previste dal Piano Triennale di Prevenzione della Corruzione, redatto dal RPCT), finalizzate a prevenire i fenomeni corruttivi e altre attività criminose nel Comune di Arnesano.
Le tutele previste dall'art. 54-bis del D.Lgs. n.165/2001 si applicano, infatti, oltre che ai dipendenti del Comune, anche ai lavoratori e collaboratori delle imprese fornitrici di beni e servizi che realizzano opere in favore del Comune, ai tirocinanti o altri soggetti che collaborano con l'Ente, nel caso in cui tali soggetti segnalino illeciti di cui siano venuti a conoscenza, in ragione del loro rapporto con il medesimo Ente.

Quali sono le responsabilità connesse al trattamento?

I soggetti coinvolti nell'attività di trattamento sono:
a) Comune di Arnesano, Titolare del trattamento;
b) RPCT interno, specificatamente designato e autorizzato al trattamento dei dati derivante dalle segnalazioni;
b) Whistleblowing Solutions, che svolge il ruolo di Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing (gestione della piattaforma e, nello specifico, per l'esecuzione di operazioni informatizzate di trattamento di dati personali relative alla raccolta e alla conservazione dei dati necessari per l'erogazione del servizio);
c) Seeweb, che svolge il ruolo di Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura (IaaS) – ARCHIVIAZIONE HOSTING CLOUD IASS;
d) Transaparency International Italia, che svolge il ruolo di Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing (SUPPORTO UTENTI e AMMINISTRATORE DI SISTEMA).

Ci sono standard applicabili al trattamento?

Nel trattamento oggetto di valutazione non ci sono specifici standard applicabili al trattamento.
I principali standard sono collegati alle caratteristiche tecniche/tecnologiche dei prodotti. Dal punto di vista del processo/trattamento e degli adempimenti conseguenti, si fa riferimento principalmente a:
- Linee guida dell'ANAC sul Whistleblowing;
- Reg. UE 2016/679 (GDPR) e D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018);
- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni basati sulla per i servizi Cloud
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud
- Qualifica AGID del fornitore
- Certificazione CSA Star.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I dati trattati consistono in operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari alla gestione delle segnalazioni (mediante un servizio erogato da terzi in modalità SaaS). Nello specifico, si tratta di:
- Dati di registrazione (dati identificativi e di contatto del referente del Titolare che attiva il servizio di digital whistleblowing, nella figura del Responsabile Anticorruzione);
- Categorie particolari di dati (dati eventualmente contenuti nelle segnalazioni e in atti e documenti allegati);
- Dati relativi a condanne penali e reati (eventualmente contenuti nella segnalazione e in atti e documenti allegati).

Il Whistleblower, in ogni caso, deve fornire tutti gli elementi utili affinché il RPCT possa procedere alle verifiche ed agli accertamenti a riscontro della fondatezza dei fatti posti alla sua attenzione.
A tale scopo, la segnalazione può contenere anche i seguenti elementi:
- L'identità del soggetto che effettua la segnalazione;
- La sua qualifica o posizione professionale;
- La data/periodo in cui si è verificato il fatto;
- Il luogo fisico in cui si è verificato il fatto;
- La natura delle azioni od omissioni commesse o tentate;
- La descrizione chiara e completa dei fatti oggetto di segnalazione;
- Le generalità o gli altri elementi che consentano di identificare il soggetto che ha posto in essere il fatto segnalato;
- L'indicazione di altri eventuali soggetti a conoscenza del fatto e/o in grado di riferire sul medesimo;
- Eventuali documenti a sostegno della segnalazione (che possono contenere ulteriori dati personali).

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

L'ordinario ciclo di vita del trattamento è sostanzialmente dato da:
- RACCOLTA DEI DATI (principalmente automatizzata)
- REGISTRAZIONE E CONSERVAZIONE (principalmente automatizzata, mediante acquisizione e caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti)
- ELABORAZIONE (TRAMITE PERSONALE ESPRESSAMENTE AUTORIZZATO)
- ARCHIVIAZIONE PER I TEMPI DEL PROCEDIMENTO IN ESSERE
- DISTRUZIONE/CANCELLAZIONE.

All'interno della piattaforma il ciclo di vita è il seguente:
- Attivazione della piattaforma
- Configurazione della piattaforma
- Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse da parte dei riceventi preposti
- Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge perfinalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore.

Quali sono le risorse di supporto ai dati?

Il Comune di Arnesano ha aderito al progetto WhistleblowingPA di Transparency International Italia e del Centro Hermes per la Trasparenza e i Diritti Umani e Digitali e ha adottato la piattaforma informatica prevista per adempiere agli obblighi normativi e in quanto ritiene importante dotarsi di uno strumento sicuro per le segnalazioni.
L'architettura di sistema è principalmente composta da:
- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

Software impiegato: Software di whistleblowing professionale GlobaLeaks
La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di Progetto.
In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile.
Vengono utilizzate (anche in modo limitato) alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.
Vengono primariamente utilizzati le seguenti tecnologie open source:
● Debian/Linux (principale sistema operativo utilizzato);
● Postfix (mail server);
● Bind9 (dns server);
● OPNSense (firewall);
● OpenVPN (vpn).

Infrastruttura IaaS e SaaS privata basata su tecnologie:
- Dettaglio Hardware
- VMWARE (software di virtualizzazione)
- Debian Linux LTS (sistema operativo)
- VEEAM (software di backup)
- OPNSENSE (firewall)
- OPENVPN (vpn)
- Plesk, software per realizzazione siti web di facciata del progetto.

Predisposizione dei sistemi virtualizzati:
- I server eseguono software VMware e vCenter abilitando funzionalità di High Availability;
- Su VMware vengono istanziate macchine virtuali Debian/Linux nelle sole version Long Term Support (LTS);
- Ogni macchina virtuale Debian implementa configurazione securizzata con: Full Disk Encryption (lvm/crypto), SecureBoot, Apparmor, Iptables;
- Entrambi i server fisici eseguono una macchina virtuale di Key Management System (KMS) per consentire continuità di servizio con immediato automatico riavvio dei sistemi senza intervento amministrativo anche in caso di totale fallimento di uno dei due server fisici componenti il cluster.

Servizio di Hosting
Il Servizio di Whistleblowing Digitale consiste in un sistema SaaS (Software as a Service) configurato e personalizzato. Non è previsto alcun tipo di fornitura tecnologica fisica, nè costi di licenza.
Il servizio è reso disponibile su infrastruttura ridondata di WBS. L'infrastruttura gestita cha esegue l'applicativo GlobaLeaks è accessibile tramite il dominio segnalazioni.nomecliente.it, di proprietà del cliente. L'infrastruttura è inoltre raggiungibile tramite Tor Onion Service il cui indirizzo viene fornito a seguito dell'attivazione del servizio.
Le piattaforme del progetto WhistleblowingPA si trovano sui Datacenter della società Seeweb (https://www.seeweb.it/), in particolare a Milano e. per ridondanza, presso Frosinone.

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?
Il Comune di Arnesano tratta i dati personali conferiti nella piattaforma, con modalità informatiche, per gestire la segnalazione in essa contenuta, finalizzata a prevenire i fenomeni corruttivi e altre attività criminose. Tale attività, in quanto l'Ente è vincolato al rispetto di norme di diritto pubblico, viene svolta in adempimento a specifici obblighi di legge e la liceità è data dall'art. 6 par. 1, lett. c) del GDPR, nonché per motivi di interesse pubblico rilevante. Tali scopi sono, pertanto, specifici, espliciti e legittimi.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica è rappresentata dalla previsione di cui all'art. 6 co. 1 lett. c) e all'art. 9, par. 2, lett. g) del Reg. UE 2016/679, in quanto risiede nell'adempimento a obblighi di legge (legge 190/2012, Legge 30 novembre 2017, n. 179, Art. 54-bis del decreto legislativo 30 marzo 2001, n. 165, rubricato "Tutela del dipendente pubblico che segnala illeciti") e in motivi di interesse pubblico rilevante.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. La piattaforma utilizzata è in linea con l'attuale normativa in quanto ha implementato tutte le misure tecniche e organizzative richieste dalle nuove disposizioni introdotte dal D.Lgs. 10 marzo 2023 n. 24.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

Per la registrazione e attivazione del servizio sulla piattaforma uilizzata per effettuare le segnalazioni 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 di appartenenza (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.

Il Fornitore della piattaforma WhisteblowingPA, di cui si è dotato il Comune, ha integrato alcune modifiche in modo che sia conforme alle disposizioni previste dalla nuova normative (decreto legislativo 24/2023, in attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019).
Le modifiche riguardano i seguenti aspetti:

- aggiornamento dell'ambito soggettivo del questionario con la previsione di tutte le tipologie di soggetti legittimati a inviare una segnalazione;
- aggiornamento dell'ambito oggettivo del questionario con la previsione delle nuove fattispecie di illecito previste dalla normativa;
- modifica dei termini di scadenza delle nuove segnalazioni che vengono ridotti dai 18 a 12 mesi (le segnalazioni precedenti mantengono la scadenza già assegnata); il soggetto ricevente, inoltre, può posticipare la data di scadenza sulla singola segnalazione

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.
Il trattamento, inoltre, avviene per le finalità che sono espressamente manifestate nell'informativa e nel Regolamento interno, in ossequio all'art. 5, par. 1, lett. b), del Regolamento UE 2016/679. Per tale motivo, sono trattati solo ed esclusivamente i dati personali necessari e sufficienti per il raggiungimento delle finalità alla base del trattamento così come previsto dall'art. 5, par. 1, lett. c) del predetto Regolamento europeo.
In ogni caso, viene e verrà rispettato il PRINCIPIO DELLA MINIMIZZAZIONE DEI DATI (ovvero riducendo al minimo i dati, trattando solo quelli indispensabili per perseguire le finalità), anche perché non risulta possibile (ovvero si rivela non efficace) il ricorso a strumenti e sistemi di gestione delle segnalazioni alternative.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento

I dati sono esatti e aggiornati?

L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.
I dati trattati, pertanto, sono esatti e, ove necessario, il Titolare procederà ad eventuale rivisitazione ed aggiornamento, anche in base ai principi sopra elencati.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con

cadenza annuale o biennale, salvo variazioni significative del trattamento.

Qual è il periodo di conservazione dei dati?

I dati delle segnalazioni acquisti tramite piattaforma (o in altra modalità) sono trattati per tutta la durata della gestione della segnalazione e sono conservati in conformità alle norme sulla conservazione della documentazione amministrativa (es. per il tempo necessario all'accertamento della fondatezza della segnalazione e, se del caso, all'adozione dei provvedimenti disciplinari conseguenti e/o all'esaurirsi di eventuali contenziosi avviati a seguito della segnalazione ovvero fino a un massimo di 5 anni dalla data di definizione e gestione della segnalazione).

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

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Il personale dipendente è informato tramite specifica informativa privacy reperibile nella intranet istituzionale, mentre gli interessati/utenti sono informati tramite specifica informativa pubblicata all'interno della Piattaforma e mediante link che rimanda alla sezione "Privacy" del sito web istituzionale.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Ove applicabile: come si ottiene il consenso degli interessati?

Il consenso non è la base giuridica per il trattamento in esame. Tuttavia, nei casi in cui è necessario attivare un eventuale procedimento disciplinare contro il presunto autore della condotta segnalata, l'identità del segnalante può essere rivelata solo dietro consenso di quest'ultimo.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni.

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

L'art. 2-undecies, comma 1, lett. f), del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018), afferma che "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:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; […]
f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio".
Per tale motivo, come specificato anche nell'informativa sul trattamento dei dati fornita, gli interessati, ricorrendo i presupposti e nei limiti previsti dall'art. 2-undecies, comma 1, del D.Lgs. 196/2003, hanno il diritto di chiedere al titolare del trattamento l'accesso ai dati personali. Tale diritto, tuttavia, non può essere esercitato 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 alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.
L'apposita istanza è presentata contattando il Comune di Arnesano, Responsabile della Prevenzione della Corruzione, all'indirizzo:
ufficiosegreteria@comune.arnesano.le.it - protocollo.comunearnesano@pec.rupar.puglia.it
Il diritto alla portabilità non è applicabile al trattamento in esame.

Valutazione: Accettabile

Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

L'art. 2-undecies, comma 1, lett. f), del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018), afferma che "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:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; […]
f) alla riservatezza dell'identita' del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio".
Per tale motivo, come specificato anche nell'informativa sul trattamento dei dati fornita, gli interessati, ricorrendo i presupposti e nei limiti previsti dall'art. 2-undecies, comma 1, del D.Lgs. 196/2003, hanno il diritto di chiedere al titolare del trattamento la rettifica o la cancellazione degli stessi. I diritti appena citati, tuttavia, 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 alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.
L'apposita istanza è presentata contattando il Comune di Arnesano, Responsabile della Prevenzione della Corruzione, all'indirizzo
ufficiosegreteria@comune.arnesano.le.it - protocollo.comunearnesano@pec.rupar.puglia.it

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

L'art. 2-undecies, comma 1, lett. f), del D.Lgs. 196/2003 (come modificato dal D.Lgs. 101/2018), afferma che "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:
a) agli interessi tutelati in base alle disposizioni in materia di riciclaggio; […]
f) alla riservatezza dell'identità del dipendente che segnala ai sensi della legge 30 novembre 2017, n. 179, l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio".
Per tale motivo, come specificato anche nell'informativa sul trattamento dei dati fornita, gli interessati, ricorrendo i presupposti e nei limiti previsti dall'art. 2-undecies, comma 1, del D.Lgs. 196/2003, hanno il diritto di chiedere al titolare del trattamento la limitazione del trattamento che li riguarda o di opporsi al trattamento. I diritti appena citati, tuttavia, 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 alla riservatezza dell'identità del dipendente che segnala l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio.
L'apposita istanza è presentata contattando il Comune di Arnesano, Responsabile della Prevenzione della Corruzione, all'indirizzo
ufficiosegreteria@comune.arnesano.le.it - protocollo.comunearnesano@pec.rupar.puglia.it

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

Gli accordi contrattuali sono definiti con chiarezza con le seguenti società:
- Whistleblowing Solutions in qualità di Responsabile del trattamento
- Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions
- Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions.

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati non vengono mai trasferiti al di fuori dell'Unione Europea. I dati personali, infatti sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste, pertanto, alcun trasferimento di Dati Personali verso

l'estero in paesi extra UE.

Valutazione: Accettabile
Commento di valutazione: l'analisi è ritenuta accettabile senza prescrizioni.

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/main/security/EncryptionProtocol.html

Le principali caratteristiche di sicurezza del framework sono:
● Supporto nativo per trasporto sicuro HTTPS con rating A+ da SSL Labs
● Supporto nativo a Let's Encrypt
● Piena integrazione della tecnologia Tor, stato dell'arte in materia di comunicazioni sicure ed anonime;
● Piena integrazione della tecnologia PGP come standard per la cifratura di email e file allegati;
● Firewall integrato;
● Application Sandboxing integrato;
● Completo set di funzionalità anti-DoS ed anti-Bot

Il software, inoltre, ha già ricevuto 4 analisi di sicurezza indipendenti ed è continuamente oggetto di peer-review dalla comunità di sviluppatori ed analisti indipendenti:
- https://github.com/globaleaks/GlobaLeaks/wiki/Penetration-Tests

Ai seguenti link è possibile consultate l'elenco completo delle misure di sicurezza applicate dal software Globaleaks:
- https://docs.google.com/document/u/1/d/1niYFyEar1FUmStC03OidYAIfVJf18ErUFwSWCmWBhcA/pub
- https://docs.google.com/document/u/1/d/1SMSiAry7x5XY9nY8GAejJD75NWg7bp7M1PwXSiwy62U/pub
- https://github.com/globaleaks/GlobaLeaks/wiki/Operating-system-security
- https://github.com/globaleaks/GlobaLeaks/wiki/Encryption

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento

Anonimizzazione

Vi è la possibilità di ricevere segnalazioni in forma anonima. 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 ricercar tecnologica in materia.

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del

trattamento

Controllo degli accessi logici

L'accesso applicativo è consentito a ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.
Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.
Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.
Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Tracciabilità applicata ai dati

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.

Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents.
L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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.

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti.

Minimizzazione dei dati

Come già specificato, 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.

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Lotta contro il malware

Architettura di rete

L'architettura di rete prevede un firewall perimetrale e segregazione della rete in molteplici VLAN al fine di isolare le differenti componenti secondo loro differente natura al fine di limitare ogni esposizione in caso di vulnerabilità su una singola componente.
Una VPN consente l'accesso alla gestione dell'infrastruttura a un limitato e definite insieme di amministratori di Sistema.
Ogni connessione di rete implementa TLS 1.2+.
Ogni macchina virtuale istanziata vede esposizione di rete limitata all'effettiva necessità.

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy istituzionale 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.

Valutazione: Accettabile

Commento di valutazione: Misura adeguata a contrastare i rischi previsti. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Back up

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

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento

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.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Contratto con il responsabile del trattamento

E' stato sottoscritto il contratto di nomina a Responsabile del trattamento dei dati personali ai sensi dell'art. 28 del Regolamento (EU) n. 679/2016 con il fornitore della Piattaforma per la gestione delle segnalazioni.
Il fornitore presenta garanzie sufficienti (in particolare, quanto a conoscenze specialistiche, affidabilità e risorse) e sono state comunicate le misure di sicurezza che detto sistema garantisce (misure di sicurezza tecniche e organizzative, compreso il rispetto dei principi di privacy by design e privacy by default, nel rispetto della vigente normativa).
Gli accordi contrattuali sono definiti con le seguenti società:
- Whistleblowing Solutions in qualità di Responsabile del trattamento
- Seeweb in qualità di Sub-Responsabile del trattamento nominato da Whistleblowing Solutions
- Transparency International Italia in qualità di Sub-Responsabile del trattamento nominata da Whistleblowing Solutions.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

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.

Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Tracciabilità sui sistemi

Tutti i dispositivi utilizzati quali l'applicativo GlobaLeaks, Log di sistema e Firewall sono configurati per non registrare alcun tipo di log e/o informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP e User Agents.
L'applicativo GlobaLeaks abilita la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Politica di tutela della privacy

Adeguamento continuo dell'Ente a quanto previsto dal GDPR, tra cui la nomina del DPO e il costante coinvolgimento dello stesso. All'interno dell'Ente esiste un'organizzazione idonea a guidare e verificare la protezione dei dati personali (designazione di un DPO/RPD, creazione di un gruppo di lavoro interno, presenza di designati ex art. 2-quaterdecies D.Lgs. 196/2003, etc.).
Il titolare del trattamento è dotato di una struttura tecnica-organizzativa in grado di mappare i processi inerenti il trattamento dei dati e di redigere le valutazioni di impatto nei casi previsti, porre in essere le misure di sicurezza per minimizzare i rischi di violazione, documentare le violazione dei dati personali, fornire supporto al fine di superarle o minimizzare il danno e, nei casi previsti, notificarle al Garante e comunicarle agli interessati e cooperare con l'autorità di controllo quando richiesto.

Valutazione: Accettabile

Commento di valutazione: Si consiglia di adottare un Modello di Gestione sulla Protezione dei dati (DPMS) e una serie di procedure interne (es. Regolamento per l'utilizzo degli strumenti informatici, posta elettronica e Internet, Procedura per l'esercizio dei diritti, Procedura per la gestione delle violazioni di dati personali, etc.) che consentano il corretto adempimento alle prescrizioni del GDPR. Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione delle politiche di tutela della privacy

L'Ente dispone di una base documentale che formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati (piano d'azione, revisione periodica delle politiche in materia di protezione dati, ecc.).

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione delle postazioni

L'accesso ai client è possibile con apposite credenziali personale (e relative politiche di sicurezza delle stesse).

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione dei rischi

Esiste una politica che definisce i processi volti a controllare i rischi che i trattamenti comportano per i diritti e le libertà degli interessati (censimento dei trattamenti di dati personali, dei dati trattati, dei supporti utilizzati, valutazione del rischio, definizione di misure esistenti o previste ecc.).

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Impostate corrette procedure di data breach e formazione dei soggetti autorizzati. Esiste una procedura interna e

istruzioni operative per rilevare e gestire eventi che possono influire sulle libertà e sulla riservatezza degli interessati (definizione delle responsabilità, piano di reazione, caratterizzazione delle violazioni ecc.). Il fornitore responsabile del trattamento è obbligato contrattualmente a supportare il Titolare nella gestione di ogni violazione dei dati personali (data breach), al fine di consentirgli di assolvere agli obblighi di cui agli artt. 32 - 34 del GDPR.
Anche Whistleblowing Solutions ha definito una propria procedura per la gestione delle violazioni dei dati personali.

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Gestione del personale

In presenza di differenti competenze, specificatamente attribuite ai singoli operatori, sono stati configurati diversi livelli di visibilità e trattamento delle immagini. I designati incaricati sono in possesso di credenziali di autenticazione che permettono di effettuare, a seconda dei compiti attribuiti ad ognuno, unicamente le operazioni di propria competenza.
Per quanto riguarda l'Ente e il Fornitore della Piattaforma, entrambi assicurano al proprio personale e ai collaboratori:
• la corretta informazione sui loro ruoli e responsabilità nell'ambito della sicurezza delle informazioni prima di ottenere l'accesso a sistemi informativi riservati;
• la predisposizione di linee guida/policy interne circa le norme comportamentali da tenere negli uffici relative all'ambito della sicurezza delle informazioni (es. lettere di autorizzazione e formazione su privacy e sicurezza);
• il raggiungimento di un adeguato livello di consapevolezza in materia di sicurezza delle informazioni adatto ai loro ruoli e responsabilità all'interno dell'organizzazione di appartenenza attraverso opportune campagne di sensibilizzazione e piani di formazione;
• formazione periodica.
In tal senso, l'Ente attua un programma di sensibilizzazione alla sicurezza delle informazioni e formazione sugli obblighi derivanti dal Reg. UE 2016/679, rendendo consapevoli personale e collaboratori delle loro responsabilità e degli strumenti con cui gestire queste responsabilità.

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Istruzioni per la gestione degli strumenti

Il personale preposto al trattamento dei dati viene formato sull'utilizzo degli strumenti software e hardware. Il RPCT è vincolato a uno specifico obbligo di riservatezza (circa l'indentità del soggetto segnalato o segnalante).

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Misure addizionali

Il presente documento sintetizza una serie di metodologie standard conformi con la normativa vigente in ambito nazionale ed internazionale in materia di trattamento sicuro dell'informazione, privacy e whistleblowing.
A queste si aggiunge un crescente insieme altre misure al passo con la ricerca e la tecnica in ambito di sicurezza informatica reperibile alle seguenti pagine web:
● THREAT MODEL
● APPLICATION SECURITY

Valutazione: Accettabile
Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Trasparenza nei confronti dell'interessato

Un'informativa chiara ed esaustiva (ai sensi dell'art. 13 del GDPR) viene fornita a tutti i dipendenti e agli altri soggetti che presentano segnalazioni di condotte illecite; tale documento informativo viene incluso nell'atto organizzativo adottato dal Titolare per la gestione delle segnalazioni (Regolamento interno) ed è stato pubblicato in un'apposita sezione dell'applicativo informatico utilizzato per l'acquisizione e gestione delle segnalazioni (nella pagina dedicata al whistleblowing, mediante link che rimanda a una specifica pagina web dove è presente l'informativa estesa).

Valutazione: Accettabile

Commento di valutazione: Aggiornamento almeno con cadenza annuale o biennale, salvo variazioni significative del trattamento.

Metodo adottato per l'analisi dei rischi

Il modello scelto per quantificare i rischi è quello della misurazione dell'esposizione al rischio:

Esposizione = probabilità x danno

La valutazione del rischio è data dalla combinazione di due parametri, ai quali si attribuisce un valore numerico a seconda della loro valutazione qualitativa. Al fine di oggettivare tale valutazione, si è adottata la metrica proposta da ENISA nel documento "Handbook on Security of Personal Data Processing":

- **gravità del rischio**, intesa come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali agli stessi derivanti dal verificarsi dell'evento considerato a rischio (la gravità del rischio può essere Bassa [1], Media [2], Alta [3], Significativa [4]). I 4 livelli di impatto si possono così descrivere:
  - Bassa [1]: Le persone possono incontrare alcuni piccoli inconvenienti, che supereranno senza problemi (tempo speso per reinserire le informazioni, fastidi, irritazioni, ecc.).
  - Media [2]: Gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà (costi extra, rifiuto di accesso ai servizi Enteli, paura, mancanza di comprensione, stress, disturbi fisici minori, ecc.).
  - Alta [3]: Gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (appropriazione indebita di fondi, inserimento nella lista nera da parte di istituzioni finanziarie, danni alla proprietà, perdita del lavoro, mandato di comparizione, peggioramento della salute, ecc.).
  - Significativa [4]: Gli Individui possono subire conseguenze significative o addirittura irreversibili, che potrebbero non superare (incapacità lavorativa, disturbi psicologici o fisici a lungo termine, morte, ecc.).
- **probabilità di accadimento** della minaccia rilevata, sulla base della natura delle minacce, delle fonti di rischio e delle misure esistenti o pianificate (la probabilità può essere Improbabile [1], Bassa [2], Media [3], Alta [4]). I 4 livelli di probabilità di accadimento si possono così descrivere:
  - Improbabile [1]: Appare impossibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Bassa [2]: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Media [3]: Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.
  - Alta [4]: Appare estremamente probabile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Viene pertanto identificata l'esposizione al rischio, intesa come combinazione moltiplicativa dei due fattori, da cui vengono stabilite le azioni da compiere sulla base della seguente tabella:

Probabilità	Alta	4	4	8	12	16
	Media	3	3	6	9	12
	Bassa	2	2	4	6	8
	Improbabile	1	1	2	3	4
			1	2	3	4
			Bassa	Media	Alta	Significativa
			Gravità			

Le azioni consequenziali da intraprendere sono le seguenti:

Livello di esposizione	Intervallo di valori	Intervento previsto
Minimo	1-3	Da Monitorare
Medio	4-8	Implementare le misure previste entro l'anno
Significativo	9-16	Intervento urgente

Accesso illegittimo ai dati

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

- Demansionamento del lavoratore, mobbing o licenziamento del dipendente
- Perdita di riservatezza sull'identità del segnalante e della segnalazione
- Misure ritorsive o discriminatorie nei confronti del lavoratore (adottate dall'Ente a causa della segnalazione effettuata) e compromissione dell'esercizio delle funzioni proprie del lavoratore (con intento vessatorio o comunque tale da peggiorare la sua situazione lavorativa);
- Danno (anche di natura economica) da trattamento illecito/non corretto (danno economico o sociale)
- Divulgazione illecita di dati personali
- Ricatto
- Discriminazione e/o stigmatizzazione
- Conoscenza di dati da parte di terzi non autorizzati.

Quali sono le principali minacce che potrebbero concretizzare il rischio?

- decifratura non autorizzata dei dati
- attacchi informatici
- accesso abusivo ai sistemi informatici
- abusi di privilegi di accesso o utilizzo improprio
- errori nei processi di elaborazione
- perdita dati per guasto/furto/smarrimento hardware (es. perdita dei dati dovuti al furto del DVR, server o delle schede dove sono memorizzate le immagini degli interessati)
- inefficiente gestione del dato
- raccolta ingiustificata o eccessiva di dati
- uso improprio o abuso dei dati (es. uso dei dati oltre le ragionevoli aspettative degli individui, l'uso insolito di dati oltre le norme dell'Ente)
- perdita o furto o distruzione e alterazione dei dati
- accesso illegittimo al sistema informativo e ai dati (perdita di confidenzialità)
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- accesso non autorizzato o accesso improprio degli autorizzati
- intercettazione
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- malware
- violazione dell'obbligo di segretezza da parte del personale preposto (es. RPCT).

Quali sono le fonti di rischio?

Fonte umana esterna intenzionale, Fonte umana interna intenzionale.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Tracciabilità sui sistemi, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione delle postazioni, Gestione dei rischi, Gestione del personale, Istruzioni per la gestione degli strumenti, Misure addizionali.

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

ALTA: I DATI TRATTATI SONO RILEVANTI, ANCHE SE I MECCANISMI DI FUNZIONAMENTO DELLA PIATTAFORMA E LE MISURE DI PROTEZIONE ADOTTATE RENDONO LA GRAVITA' DEL RISCHIO NON MASSIMA.

Appare possibile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate. Gli interessati potrebbero sperimentare inconvenienti significativi, ma superabili.

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

BASSA: Appare difficile che le fonti di rischio considerate concretizzino una minaccia sulla base della situazione di contesto e delle misure adottate.

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
3	2	6	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale.

Valutazione: Accettabile

Commento di valutazione: è opportuno un allineamento e aggiornamento delle procedure interne dell'Ente sul processo di segnalazione alla recente normativa nazionale (D.Lgs. n. 24/2023) e una specifica formazione per il RPCT interno all'Ente circa il rispetto delle prescrizioni in materia di data protection (anche in termini di istruzioni ai soggetti autorizzati al trattamento circa gli obblighi di riservatezza o procedure per la raccolta del consenso espresso del segnalante nel caso di registrazioni delle segnalazioni mediante sistemi di chiamata, messaggistica vocale o di supporti di registrazione).

Modifiche indesiderate dei dati

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

- Danno da trattamento illecito/non corretto (danno economico o sociale)
- Divulgazione di dati personali modificati
- Errata gestione della segnalazione
- Danni alla capacità di guadagno e perdite finanziarie
- Impedimento dell'esercizio del controllo sui dati personali o limitazione dei diritti
- Lesione di un diritto fondamentale dell'interessato, del diritto a difendersi in giudizio o a esercitare un diritto in sede giudiziaria (contro i fenomeni corruttivi e altre attività criminose).

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

- errata elaborazione dei dati o inefficiente gestione del dato
- attacchi informatici
- accesso abusivo ai sistemi informatici
- abusi di privilegi di accesso o utilizzo improprio
- errori nei processi di elaborazione
- alterazione dei dati illecita o non autorizzata
- alterazione delle impostazioni di funzionamento della Piattaforma
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- accesso non autorizzato o accesso improprio degli autorizzati
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- malware
- danneggiamento degli hardware o dei software dell'impianto
- uso o conservazione dei dati inesatti o non aggiornati.

Quali sono le fonti di rischio?

- Fonte umana esterna intenzionale, Fonte umana interna intenzionale.

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

Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Back up, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Tracciabilità sui sistemi, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione delle postazioni, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Istruzioni per la gestione degli strumenti, Misure addizionali, Trasparenza nei confronti dell'interessato.

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

ALTA: gli individui possono incontrare conseguenze significative, che dovrebbero essere in grado di superare anche se con gravi difficoltà (il rischio riguarda principalmente i trattamenti errati derivanti da zioni umane che

potrebbero portare a conseguenti elaborazioni errate dei dati, da attacchi informatici, o malware ovvero da guasti hardware o software).

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

IMPROBABILE: LE MISURE ADOTTATE RENDONO LA PROBABILITA' DI RISCHIO MOLTO LIMITATA. Appare altresì difficile che si realizzi una modifica indesiderata dei dati in questione, considerando le misure adottate e le garanzie fornite dalla Piattaforma.

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
3	1	3	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale

Valutazione: Accettabile

Perdita di dati

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

- Lesione dei diritti fondamentali degli interessati
- Danno da trattamento illecito/non corretto (danno economico o sociale)
- Danni alla capacità di guadagno e perdite finanziarie
- Impedimento dell'esercizio del controllo sui dati personali o limitazione dei diritti
- Lesione del diritto a difendersi in giudizio o a esercitare un diritto in sede giudiziaria ovvero impossibilità di risalire a condotte illecite (es. fenomeni corruttivi e altre attività criminose).

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

- attacchi informatici al sistema
- cancellazione accidentale
- abusi di privilegi di accesso o utilizzo improprio
- accesso abusivo ai sistemi informatici
- errori nei processi di elaborazione
- inefficiente gestione del dato
- perdita, furto o distruzione dei dati
- comportamento illecito/illegittimo degli utenti, operatori o amministratori di sistema
- accesso non autorizzato o accesso improprio degli autorizzati
- attacchi al sistema di autenticazione o variazione non autorizzata delle credenziali di accesso al sistema informativo
- malware
- malfunzionamenti/danni infrastrutturali.

Quali sono le fonti di rischio?

- Fonte umana esterna intenzionale, Fonte umana interna intenzionale.

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

Controllo degli accessi logici, Tracciabilità applicata ai dati, Archiviazione, Minimizzazione dei dati, Vulnerabilità, Lotta contro il malware, Back up, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dei canali informatici, Tracciabilità sui sistemi, Politica di tutela della privacy, Gestione delle politiche di tutela della privacy, Gestione delle postazioni, Gestione dei rischi, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Istruzioni per la gestione degli strumenti, Misure addizionali.

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

MEDIA: nonostante le misure adottate, gli individui possono incontrare notevoli inconvenienti, che saranno in grado di superare nonostante alcune difficoltà.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle

fonti di rischio e alle misure pianificate?

IMPROBABILE: LE MISURE ADOTTATE SONO EFFICACI.

Livello di esposizione al rischio

GRAVITA'	PROBABILITA'	ESPOSIZIONE	INTERVENTO PREVISTO
2	1	2	Nessun intervento previsto. Le misure di sicurezza individuate e applicate consentono una riduzione importante del rischio finale

Valutazione: Accettabile

Commento di valutazione: appare non molto probabile che le fonti di rischio considerate concretizzino una minaccia e le misure di sicurezza adottate consentono di considerare "minimo" il livello di materializzazione del rischio.

Piano d'azione

Principi fondamentali

SI	ACC	MIG	ELENCO PRINCIPI
X	X		Finalità
X	X		Basi legali
X	X		Adeguatezza dei dati
X	X		Esattezza dei dati
X	X		Periodo di conservazione
X	X		Informativa
n/a	-		Raccolta del consenso
X	X		Diritto di accesso e portabilità dei dati
X	X		Diritto di rettifica e diritto di cancellazione (ove compatibili il perseguimento delle finalità di pubblico interesse come previsto dall'art. 6 par. 1 lett. e), del GDPR)
X	X		Diritto di limitazione e diritto di opposizione (ove compatibili finalità di pubblico interesse come previsto dall'art. 6 par. 1 lett. e), del GDPR)
X	X		Responsabili del trattamento
X	X		Trasferimenti di dati

ACC: Principi valutati Accettabili

MIG: Principi valutati Migliorabili

Piano d'azione

Aggiornamento del Regolamento o delle procedure interne dell'Ente sul Whistleblowing alla nuova normativa nazionale appena entrata in vigore; in particolare al Decreto Legislativo 10 marzo 2023, n. 24 (c.d. Decreto Whistleblowing) di recepimento della Direttiva UE 23 ottobre 2019, n. 1937 e alle prescrizioni di cui alle Linee Guida ed altri atti di indirizzo adottati dall'Autorità Nazionale Anticorruzione (A.N.A.C.) in materia.

Misure esistenti e pianificate

SI	ACC	MIG	ELENCO MISURE
X	X		Crittografia
X	X		Anonimizzazione
X	X		Controllo degli accessi logici
X	X		Tracciabilità applicata ai dati
X	X		Archiviazione
X	X		Minimizzazione dei dati
X	X		Vulnerabilità
X	X		Lotta contro il malware
X	X		Back up
X	X		Manutenzione
X	X		Contratto con il responsabile del trattamento

X	X		Sicurezza dei canali informatici
X	X		Tracciabilità sui sistemi
X	X		Gestione delle politiche di tutela della privacy
X	X		Gestione delle postazioni
X	X		Gestione dei rischi
X	X		Gestire gli incidenti di sicurezza e le violazioni dei dati personali
X	X		Gestione del personale
X	X		Istruzioni per la gestione degli strumenti
X	X		Misure addizionali
X	X		Trasparenza nei confronti dell'interessato

ACC: Misure valutate Accettabili

MIG: Misure valutate Migliorabili

Piano d'azione

Definire un piano di formazione specifica per il personale addetto alla gestione delle segnalazioni (es. per il RPCT).

Rischi

SI	ACC	MIG	ELENCO RISCHI
X	X		Accesso illegittimo ai dati
X	X		Modifiche indesiderate dei dati
X	X		Perdita dei dati

ACC: Principi valutati Accettabili

MIG: Principi valutati Migliorabili

Piano d'azione

Monitorare periodicamente l'efficacia delle misure tecniche adottate dal fornitore e quelle organizzative interne.

Pareri

Parere DPO/RPD

L'Avv. Marco Micella, nella qualità di Responsabile della Protezione Dati dell'Ente, ha espresso il seguente parere:

"*In seguito ad attenta analisi del presente documento, visto l'art. 39 par. 1 lett. c) del Reg. UE 2016/679, 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 degli interessati, rispetto alle finalità di rilevante interesse pubblico perseguite e in adempimento a specifici requisiti di legge.*

Nello specifico, sembrano rispettate tutte le indicazioni del Garante per la protezione dei dati personali e dalle Linee Guida dell'ANAC a tutela dei dati personali trattati.

Pertanto nel complesso, alla data odierna e alla luce delle misure di sicurezza tecniche e organizzative adottate, si concorda sul fatto che non vi sia 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.

In qualità di DPO, tuttavia, consiglio di monitorare e verificare periodicamente le misure di sicurezza logiche e organizzative implementate, nonché vigilare sul rispetto delle istruzioni date ai soggetti autorizzati al trattamento, in quanto il fattore umano può costituire l'anello debole della catena che mette a rischio la sicurezza e la riservatezza dell'intero processo delle segnalazioni".

Parere degli interessati

Non è stato possibile acquisire il parere degli interessati in quanto la platea dei potenziali interessati è ampia e indeterminabile; ciò rende particolarmente difficile eseguire una tale richiesta, anche perché il trattamento oggetto di analisi è svolto per il perseguimento di determinate finalità in precedenza indicate e nell'adempimento a uno specifico

obbligo di legge (e di regolamento interno). Inoltre, acquisire un parere di un soggetto che potrebbe potenzialmente essere un soggetto segnalato, non sarebbe obiettivo e realmente utile allo scopo della presente valutazione d'impatto, in quanto sarebbe inficiato da personali valutazioni opportunistiche.