C O M U N E D I C O R A T O

Valutazione d'impatto sulla protezione dei dati personali trattati nella gestione delle segnalazioni di violazioni (cd. whistleblowing) attraverso l'utilizzo del canale interno – art. 13 d.lgs. 24/2023

Sommario

1. Premesse e normativa di riferimento 3
2. Valutazione preliminare: necessità di condurre un'attività di DPIA 4
3. Descrizione del trattamento 5
3.1 Informazioni chiave 5
3.2 Descrizione del sistema utilizzato e flusso dei dati personali 8
4. Principi fondamentali 14
5. Misure previste per affrontare il rischio 15
6. Conclusioni 22
7. Parere del DPO 25

1. Premesse e normativa di riferimento

Il presente documento è stato redatto in conformità a quanto previsto dall'articolo 35 "*Valutazione d'impatto sulla protezione dei dati*" del Regolamento **UE/679/2016** del Parlamento Europeo e del Consiglio, **Regolamento Generale sulla protezione dei dati**, adottato il 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE, nonché alla luce delle **Linee Guida pubblicate in materia dal Garante per la protezione dei dati personali in data 4 aprile 2017 (WP248)**, successivamente modificate e adottate in data 4 ottobre 2017. Le appena citate Linee Guida, tengono conto dei seguenti documenti:

a. dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati – dichiarazione del WP29 14/EN WP 218 sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, adottata il 30 maggio 2014;

b. linee guida sui responsabili della protezione dei dati del WP29-16/EN WP 243, adottate il 13 dicembre 2016;

c. parere del WP29 sulla limitazione delle finalità- 13/EN WP 203, approvato il 2 aprile 2013;

d. norme internazionali (ad esempio, la norma ISO 31000:2009 *et similia*).

La *Data Protection Impact Assessment* (di seguito, per brevità, DPIA) può essere definita come un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche, derivanti dal trattamento di dati personali, valutando detti rischi e determinando misure per affrontarli. In altre parole, in accordo con quanto previsto dall'articolo 24 del Regolamento, la DPIA è uno strumento indispensabile per il Titolare del Trattamento, dal momento che lo sostiene non solo nel rispettare i requisiti dettati dal GDPR, ma anche nel dimostrare che sono state adottate tutte le misure necessarie a garantire tale rispetto.

Nonostante l'importanza di questo strumento, la DPIA non risulta necessaria per qualsiasi attività di trattamento. Infatti, in ossequio a quanto previsto dal paragrafo 1 dell'art. 35, **il titolare dovrà procedere con tale valutazione solo quando il trattamento, prevedendo l'uso di nuove tecnologie e tenuto conto della natura, dell'oggetto, del contesto e delle finalità dello stesso, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche** (i.e. diritto alla privacy, libertà di pensiero, diritto alla parola, libertà di circolazione, diritto alla libertà di coscienza e religione e similari).

2. Valutazione preliminare: necessità di condurre un'attività di DPIA

Con riferimento al trattamento di dati personali nell'ambito della gestione delle segnalazioni di violazioni (cd. whistleblowing) l'**obbligo di condurre una valutazione di impatto** è previsto espressamente dall'**art. 13 del decreto legislativo n. 24/2023**. Per capire quali siano le caratteristiche del trattamento in esame che giustifichino la necessità di condurre una DPIA, è utile il riferimento alle "*Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679*" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 4 aprile 2017, come modificate e adottate da ultimo il 4 ottobre 2017 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "**WP 248, rev. 01**") considerate le quali, il Garante Privacy Italiano ha emanato, l'11 ottobre 2018, l' "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35, comma 4, del Regolamento (UE) n. 2016/679*".

In particolare, le LG **WP 248, rev. 01** hanno individuato nove criteri da tenere in considerazione ai fini dell'identificazione dei trattamenti che possono presentare un "rischio elevato" e che necessitano, pertanto, di una valutazione d'impatto. Con particolare riferimento all'attività di trattamento in esame, tra i nove criteri considerati, rilevano i seguenti:

- criterio di cui al punto 7 - **dati relativi a interessati vulnerabili** (considerando 75): *il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento*;
- criterio di cui al punto 4 - **dati sensibili o dati aventi carattere altamente personale**: *questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10 (..). Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato*;

- criterio di cui al punto 9 - quando il trattamento in sé "impedisce agli interessati di esercitare un diritto (..)". Sul punto, è lo stesso d.lgs. 24/2023 che prevede che la segnalazione non può essere oggetto di accesso documentale e accesso civico di cui, rispettivamente agli articoli 22 e ss. L. 241/1990 e artt. 5 e ss. D.lgs. 33/2013. Anche i diritti in materia di protezione dei dati personali di cui agli artt. 15 e 22 subiscono le limitazioni previste dall'articolo 2-undecies del D.lgs. n. 196/2003 e s.m.i..

3. Descrizione del trattamento

Di seguito, dopo una tabella recante indicazione delle informazioni fondamentali del trattamento in esame, verrà descritto il ciclo di vita dei dati oggetto di trattamento, descrizione necessaria per avere una precisa comprensione dell'impiego dei dati e dei rischi ai quali essi sono esposti.

3.1 Informazioni chiave

(a)	Titolare del Trattamento	**Comune di Corato**
(b)	Descrizione del trattamento	Attività di ricezione e gestione delle segnalazioni di violazioni (cd. whistleblowing) attraverso il canale interno di segnalazione (progetto Whistleblowing PA).
(c)	Finalità del trattamento	L'attività di trattamento su descritta è necessaria al fine di: - svolgere l'attività istruttoria volta a verificare la fondatezza della segnalazione ricevuta, nonché - adottare gli eventuali provvedimenti conseguenti che si rendano necessari.

(d)	Dati personali oggetto di trattamento	L'attività in oggetto comporta il trattamento delle seguenti categorie di dati personali: COMUNI: dati anagrafici (cognome e nome, data di nascita, luogo di nascita, codice fiscale, altro...); Dati di contatto (indirizzo postale o di posta elettronica, numero di telefono fisso o mobile); ruolo lavorativo ricoperto, condizioni personali. CATEGORIE PARTICOLARI: nelle segnalazioni effettuate nonché nella documentazione allegata, il segnalante può indicare dati personali "particolari" riferiti a sé stesso o ai soggetti coinvolti nella segnalazione. RELATIVI A CONDANNE PENALI E REATI: sempre contenuti nella segnalazione e/o nella documentazione allegata.
(e)	Base giuridica del trattamento	- il trattamento dei **dati "comuni"** si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c) del GDPR), nonché sull'esecuzione di compiti di interesse pubblico assegnati dalla legge all'Agenzia delle entrate (art. 6, par. 1, lett. e) del GDPR), nonché sul par. 2 e 3 del medesimo articolo; - il trattamento dei **dati appartenenti a categorie particolari** si fonda sull'assolvimento di obblighi e sull'esercizio di diritti specifici del Titolare del trattamento e dell'interessato in materia di diritto del lavoro (art. 9, par. 2, lett. b), GDPR), nonché sull'esecuzione di un compito di interesse pubblico rilevante (art. 9, par. 2, lett. g), GDPR), in ragione dell'art. 2-sexies lett. dd) del D.lgs. 196/2003;

		- il trattamento di **dati relativi a condanne penali e reati**, tenuto conto di quanto disposto dall'art. 10 GDPR, si fonda sull'obbligo di legge a cui è soggetto il Titolare del trattamento (art. 6, par. 1, lett. c), GDPR) e sull'esecuzione di compiti di interesse pubblico (art. 6, par. 1, lett. e), GDPR), in ragione dell'art. 2-octies par. 3 lett. a) del D.lgs. 196/2003. I trattamenti necessari per l'esecuzione di compiti di interesse pubblico sono legittimati dall'osservanza della disciplina di settore (in particolare L. 179/2017, D.lgs. 24/2023 recante "attuazione della Direttiva UE 2019/1937") secondo quanto previsto dagli artt. 2 ter e 2 sexies del d.lgs. 196/2003 – Codice Privacy.
(f)	Destinatari dei dati raccolti	- internamente all'Ente: Responsabile della Prevenzione della Corruzione e della Trasparenza e, in casi eccezionali, uno o più soggetti formalmente autorizzati al trattamento e specificamente formati. - esternamente all'Ente: i dati vengono trattati da soggetti terzi che agiscono in qualità di Responsabili/Sub-Responsabili del trattamento, formalmente nominati ai sensi dell'art. 28 GDPR. Con particolare riferimento alla piattaforma utilizzata, il Comune ha nominato "Responsabile del Trattamento" la società Whistleblowing Solutions I.S. S.r.l., fornitrice della piattaforma, la quale, a sua volta ha nominato "sub-responsabili del trattamento" le società Seeweb S.r.l., per la gestione dell'infrastruttura (iaas) e Transparency International Italia, per la collaborazione nella gestione del sistema whistleblowing.

3.2 Descrizione del sistema utilizzato e flusso dei dati personali

Il Comune di Corato, per la gestione delle segnalazioni interne whistleblowing ha aderito al progetto Whistleblowing PA, progetto nato dalla volontà di Transparency International Italia e di Whistleblowing Solutions Impresa Sociale, che ha messo a disposizione di tutte le PA un software, basata sul software GlobaLeaks, che permette al Responsabile per la Prevenzione della Corruzione e all'ulteriore personale eventualmente preposto a gestire l'attività, di ricevere le segnalazioni di illeciti da parte dei dipendenti dell'ente e di dialogare con i segnalanti, anche in modo anonimo.

Si riportano, di seguito, alcune caratteristiche tecniche del sistema utilizzato, fornite direttamente dalla società Whistleblowing Solutions I.S. S.r.l. nell'ambito del "*Documento a supporto del titolare per la valutazione d'impatto sulla protezione dei dati*" aggiornato l'11 gennaio 2023.

ARCHITETTURA DI SISTEMA

L'architettura di sistema è principalmente composta da:

- Un cluster di due firewall perimetrali;
- Un cluster di due server fisici dedicati;
- Una Storage Area Network pienamente ridondata.

SOFTWARE IMPIEGATO

La piattaforma informatica di segnalazione è basata sul software libero ed open-source GlobaLeaks di cui Whistleblowing Solutions è co-autore e coordinatore di progetto. In aggiunta a GlobaLeaks, utilizzato in via principale per l'implementazione del servizio, per finalità di pubblicazione, documentazione e supporto del progetto vengono utilizzate altre tecnologie a codice aperto e di pubblico dominio la cui qualità è indipendentemente verificabile.

Vengono anche in modo limitato utilizzate alcune note tecnologie proprietarie e licenziate necessarie per finalità di gestione infrastrutturale e backup professionale.

Vengono primariamente utilizzati le tecnologie open source:

- Debian/Linux (principale sistema operativo utilizzato);
- Postfix (mail server);
- Bind9 (dns server);
- OPNSense (firewall);
- OpenVPN (vpn).

Le limitate componenti software di natura proprietaria impiegate sono le seguenti:

- VMware, software di virtualizzazione;
- Veeam, software di backup;
- 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.

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 definito 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 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.

Al sistema sono applicabili i seguenti standard di conformità normativa:

- ISO27001 "Erogazione di Servizi SaaS di Whistleblowing Digitale su base GlobaLeaks"
- ISO27017 controlli di sicurezza sulle informazioni per i servizi Cloud;
- ISO27018 per la protezione dei dati personali nei servizi Public Cloud;
- Qualifica AGID;
- Certificazione CSA Star.

Flusso dei dati personali

Il segnalante accederà alla piattaforma attraverso apposito link posto in calce alla home page del sito istituzionale e potrà inviare una nuova segnalazione oppure accedere alla segnalazione già effettuata per monitorarne lo stato di avanzamento o per interloquire con il RPCT e l'eventuale altro personale preposto.

Il sistema prevede sia la possibilità di segnalazioni anonime che di segnalazioni riservate. Contestualmente all'apertura della segnalazione il segnalante ha la possibilità di scegliere se fornire la propria identità indicando il proprio nome, cognome ed un eventuale metodo di contatto alternativo alle comunicazioni via piattaforma. Se non fornita, il segnalante può a sua scelta decidere di comunicare la propria identità successivamente in fase di integrazione della segnalazione.

In ogni situazione in cui il segnalante abbia inserito queste informazioni a sistema, i riceventi hanno la possibilità di vedere se questa sia presente e la possibilità di richiederne accesso tramite un pulsante "Mostra". Tali informazioni identificative del segnalante sono visualizzabili in una apposita sezione separata dai contenuti della segnalazione.

Per inviare una nuova segnalazione, il segnalante dovrà compilare un questionario, fornendo le seguenti informazioni:

WHISTLEBLOWINGPA

Corato

1 Informazioni Preliminari | 2 Compila La Tua Segnalazione | 3 Passo Conclusivo

La tua segnalazione si riferisce all'ente pubblico o a un'azienda partecipata o controllata dallo stesso? *

Ente pubblico

Che rapporto hai con l'ente oggetto della segnalazione? *

Seleziona un'opzione

Hai già segnalato internamente all'ente? *

Seleziona un'opzione

Hai già segnalato o denunciato a Procura, forze dell'ordine o ANAC? *

Seleziona un'opzione

Hai subito discriminazioni o ritorsioni in seguito a segnalazioni interne o esterne già effettuate? *

Tieni presente che, se vuoi comunicare di aver subito ritorsioni e non anche inviare una segnalazione di illeciti, questa comunicazione deve essere inviata all'Autorità Nazionale Anticorruzione (ANAC).

Seleziona un'opzione

Successivo

WHISTLEBLOWINGPA

Corato

1 Informazioni Preliminari | 2 Compila La Tua Segnalazione | 3 Passo Conclusivo

La tua identità non può essere rivelata. Nel caso sia necessario utilizzare la tua segnalazione, e quindi il tuo nome, per un procedimento disciplinare, dovrà essere richiesto il tuo consenso.
Ti verranno inviate risposte alla segnalazione e richieste di chiarimenti esclusivamente su questa piattaforma, a meno che indichi diversi metodi di contatto.

Vuoi dirci chi sei?

(•) Si ( ) No

Nome *

Cognome *

Metodo di contatto alternativo *

Seleziona un'opzione

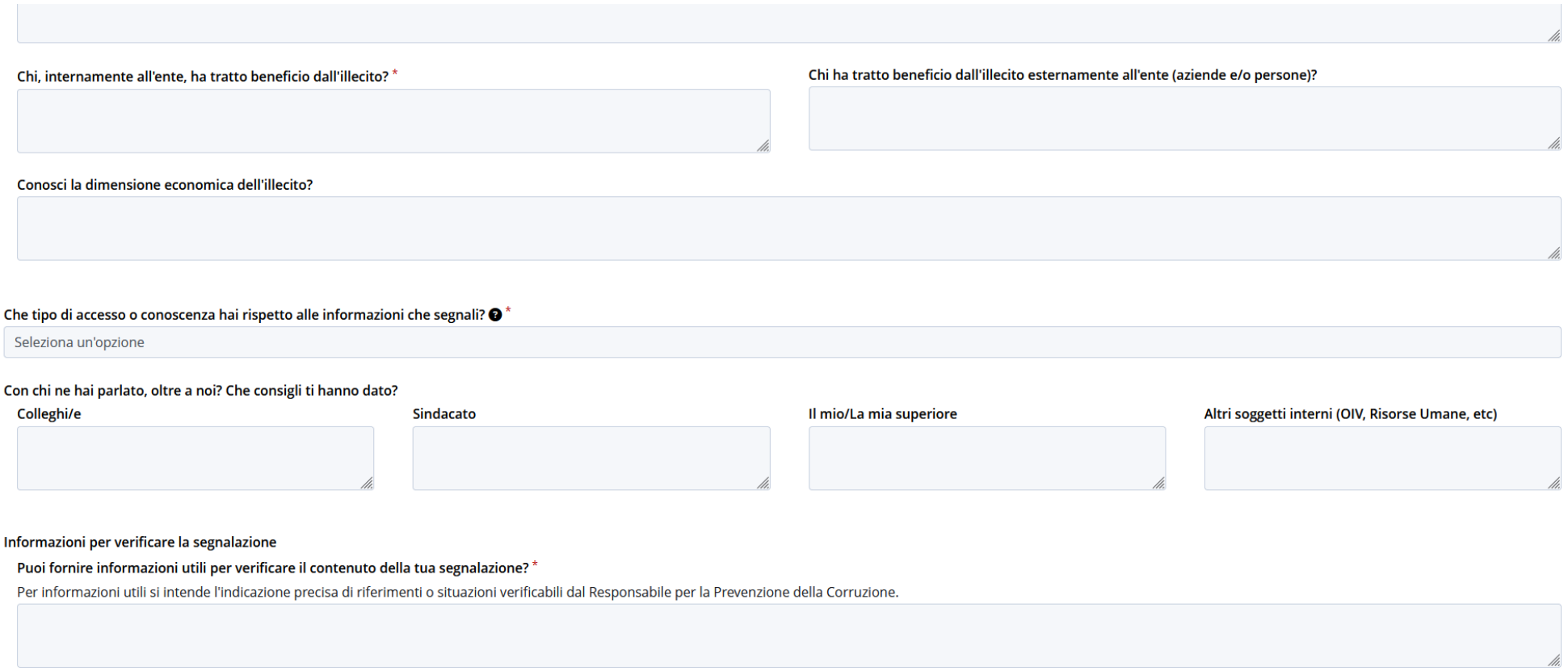
Che tipo di illecito vuoi segnalare? *

Puoi anche indicare più di un illecito ma è suggerita la maggior precisione possibile per agevolare l'inquadramento dei fatti.

- [ ] Illecito amministrativo
- [ ] Illecito contabile
- [ ] Illecito civile
- [ ] Illecito penale
- [ ] Violazione di norme comunitarie

Descrizione dei fatti

Descrivi quello che è successo in modo sintetico (massimo 200 caratteri) *



Una volta inviata la segnalazione, al segnalante verrà rilasciato un “key code” di 16 cifre, non riproducibile, che potrà utilizzare per accedere alla propria segnalazione nei termini sopra detti.

4. Principi fondamentali

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Nell'ambito dell'attività di trattamento in esame, i dati vengono trattati per perseguire le finalità sopra indicate, predeterminate e previste dalla specifica normativa di settore. Le finalità perseguite sono chiaramente riportate nei documenti informativi predisposti dall'Ente e resi disponibili mediante pubblicazione in apposita sezione del sito internet.

Quali sono le basi legali che rendono lecito il trattamento?

Vedasi la tabella sopra.

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

Come precisato da Whistleblowing Solutions I.S. S.r.l. nel documento sopra citato "*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*". L'Ente non chiede dati ulteriori rispetto a quelli richiesti nel questionario presente in piattaforma.

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.

I dati sono esatti e aggiornati?

L'aggiornamento dei dati e delle informazioni fornite con le segnalazioni è a cura dei segnalanti stessi. Il RPCT, (e l'eventuale personale delegato in via eccezionale), accedendo in piattaforma, avrà modo di vedere gli aggiornamenti fatti.

Qual è il periodo di conservazione dei dati?

Le segnalazioni, così come la documentazione ad esse allegata e le informazioni in esse contenute, verranno conservate in piattaforma per il tempo strettamente necessario alla gestione delle segnalazioni stesse o fino al termine del contratto sottoscritto con il fornitore della stessa. In ogni caso, come previsto dalla vigente normativa, le segnalazioni non potranno essere conservate oltre ai 5 anni successivi alla data della comunicazione dell'esito finale della procedura di segnalazione. Trascorso tale termine, come previsto nel su citato documento fornito dal fornitore, le segnalazioni e i dati in esse contenuti verranno cancellate in modo sicuro dallo stesso.

L’Ente, trascorsi i termini di cui sopra, potrà conservare le segnalazioni, in forma anonima, esclusivamente per finalità statistiche.

Come sono informati del trattamento gli interessati?

L’Ente, nel rispetto del principio di trasparenza, ha predisposto un documento informativo ad hoc per i soggetti interessati (segnalanti, segnalati, facilitatori e ogni altro soggetto coinvolto dalla segnalazione), mettendolo a disposizione sia sul sito internet, nell’apposita sezione dedicata al whistleblowing (cui si può accedere direttamente cliccando sul link posto in calce alla home page).

Come fanno gli interessati a esercitare i loro diritti?

Le informazioni relative ai diritti esercitabili dagli interessati sono riportate nel modello informativo predisposto e reso disponibile con le modalità sopra descritte.

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

Come precisato sopra, l’Ente ha individuato la società Whistleblowing Solutions I.S. S.r.l. quale “Responsabile del Trattamento” attraverso uno specifico accordo contrattuale, sottoscritto da entrambe le parti.

In caso di trasferimento dei dati al di fuori dell’Unione Europea i dati godono di una protezione equivalente?

Non sono previsti trasferimenti dei dati fuori dall’UE.

5. Misure previste per affrontare il rischio

5.1 Valutazione del Rischio

La valutazione dei rischi riflette un giudizio che nel tempo potrebbe cambiare in ragione dell’evoluzione del quadro normativo e della struttura organizzativa.

Per questo, l’Ente verifica con frequenza annuale il sistema di classificazione, di identificazione e mappatura delle aree a rischio, al fine di garantire una mappatura delle aree sensibili costantemente aggiornata.

Il modello scelto per quantificare i rischi è quello della determinazione dell’esposizione al rischio:

esposizione= probabilità x impatto

La valutazione del rischio, al lordo delle misure di sicurezza adottate, è data dalla combinazione di due coefficienti:

- **Probabilità** di accadimento della minaccia rilevata (la probabilità è legata anche all'esistenza o meno di strumenti di controllo/regole atti a prevenire il verificarsi della minaccia rilevata).
  [**TRASCURABILE**: il suo verificarsi richiederebbe la concomitanza di più eventi poco probabili/non si sono mai verificati fatti analoghi/il suo verificarsi susciterebbe incredulità; **BASSA**: il suo verificarsi richiederebbe circostanze non comuni e di poca probabilità/ si sono verificati pochi fatti analoghi/ il suo verificarsi susciterebbe modesta sorpresa; **MEDIA**: si sono verificati altri fatti analoghi/ il suo verificarsi susciterebbe modesta sorpresa; **ALTA**: si sono verificati altri fatti analoghi/ il suo verificarsi è praticamente dato per scontato]

- **Impatto** inteso come possibile effetto sulla dignità e libertà degli interessati oppure danni materiali allo stesso derivanti dal verificarsi dell'evento considerato a rischio.
  [**TRASCURABILE**: piccoli inconvenienti superabili senza particolari problemi (tempo necessario per re-inserire informazioni, ecc.); **BASSO**: Inconvenienti significativi, superabili con alcune difficoltà (costi aggiuntivi, mancato accesso a servizi aziendali, timori, difficoltà di comprensione, stress, piccoli disturbi fisici, ecc.); **MEDIO**: conseguenze significative che si dovrebbero poter superare ma con gravi difficoltà (sottrazione di liquidità, inserimento in elenchi negativi da parte di istituti finanziari, danni a beni materiali, perdita dell'impiego, ordinanze o ingiunzioni giudiziarie, compromissione dello stato di salute, ecc.); **ALTO**: conseguenze significative o irreversibili, non superabili (perdita capacità lavorativa, disturbi psicologici o fisici cronici, decesso, ecc.)]

La soglia di accettabilità del rischio è impostata a 8.

Griglia di valutazione

IMPATTO	4. Alto	4	8	12	16
	3. Medio	3	6	9	12
	2. Basso	2	4	6	8
	1. Irrilevante	1	2	3	4
		1. Irrilevante	2. Basso	3. Medio	4. Alto
		PROBABILITÀ			

Quando la valutazione del rischio nella matrice è:

verde (p*i < 6) = livello di rischio considerato accettabile;

giallo (p*i <9) = livello di rischio considerato accettabile, condizionato alla pianificazione di interventi di mitigazione entro l'anno;

rosso (p*i ≥9) = indispensabile attivare rapidamente contromisure di adeguamento.

Rischi correlati alla perdita di riservatezza, integrità e disponibilità

Di seguito riportiamo le minacce oggetto di analisi, raggruppandole in 3 macrocategorie (minacce relative al personale, minacce relative agli strumenti e minacce relative al contesto) fornendo la descrizione della fonte di rischio, sia di tipo accidentale, sia di tipo intenzionale, correlandole a conseguenze ed effetti sugli interessati.

In particolare, viene presa in considerazione la perdita di **riservatezza** (in tabella indicata come "R"), intesa come accessibilità al dato solo a soggetti autorizzati, **integrità** (in tabella indicata come "I"), intesa come esattezza e coerenza, e **disponibilità** (in tabella indicata come "D"), intesa come la possibilità, per i soggetti autorizzati, di accedere ai dati per un tempo stabilito e in modo ininterrotto.

MACROCATEGORIE	EVENTO/ MINACCIA	FONTE/ CAUSA DELL'EVENTO/ MINACCIA	CONSEGUENZE SUL DATO SICUREZZA)	MISURE DI MITIGAZIONE IN ESSERE	IMPATTO	PROBABILITA'	VALORE DEL RISCHIO	MISURE DI MITIGAZIONE DA IMPLEMENTARE
MINACCE RELATIVE AL PERSONALE	sottrazione delle credenziali di accesso al computer e alla piattaforma	errata gestione credenziali; mancata o scarsa formazione/sensibilizzazione del personale	R	adozione di un Regolamento interno /istruzioni su utilizzo credenziali; istruzione/ sensibilizzazione del personale sulla corretta conservazione delle credenziali	BASSO	1	4	ADEGUATO
	inadeguata gestione dei dati e delle informazioni da parte del personale - colloqui telefonici/trattamenti verbali	mancanza di Regolamenti/policy/istruzioni specifiche sul trattamento verbale di dati	R	adozione di un Regolamento interno contenente istruzioni/norme comportamentali per i trattamenti verbali di dati; formazione/ sensibilizzazione del personale; consegna al personale di specifici atti autorizzativi contenenti istruzioni sulle modalità di trattamento	BASSO	2	2	ADEGUATO
	uso improprio della piattaforma /abbandono della postazione senza effettuare la disconnessione dal sistema	mancata formazione/sensibilizzazione del personale - assenza o carenza di istruzioni per il trattamento dei dati	R	policy interna / Regolamento interno /istruzioni su gestione delle postazioni di lavoro; formazione del personale disattivazione schermata dopo inutilizzo/password di accesso al pc/disconnessione automatica dopo pochi minuti	BASSO	2	2	ADEGUATO

	errata gestione dei dati durante lo smartworking da tenere solo se lo smartworking è previsto da parte dei soggetti che gestiscono le segnalazioni	mancanza di Regolamenti/policy/istruzioni per il personale sul trattamento dei dati nello svolgimento dell'attività lavorativa in modalità agile	R	policy interna / Regolamento interno /istruzioni su gestione dei dati in smartworking; utilizzo dispositivi personali ma con account specifico per l'attività lavorativa e adeguatamente protetto; no utilizzo dispositivi condivisi con familiari	MEDIO	1	3	ADEGUATO
	errata gestione dei dispositivi mobili/removibili (usb, tabet, pc portatili..) e delle stampanti	mancata sensibilizzazione/formazione del personale	R D	sensibilizzazione del personale sul divieto di utilizzare dispositivi removibili personali, sulla corretta custodia degli strumenti e sulla gestione delle stampe	MEDIO	1	3	ADEGUATO
	alterazione/distruzione colposa di dati informatizzati	mancata formazione/sensibilizzazione del personale, mancato accesso ai dati da parte dei soli soggetti autorizzati, mancanza copie di backup		formazione del personale; backup remoto giornaliero con policy di data retention di 7 giorni;	BASSO	1	4	ADEGUATO
MINACCE RELATIVE AGLI STRUMENTI	accessi da parte di soggetti esterni non autorizzati - azione di programmi malevoli (virus, malware..) o ransomware/phishing	inadeguata o errata configurazione degli applicativi di protezione software (antimalware, firewall..)	R, D	i computer del fornitore responsabile del trattamento e dei sub responsabili eseguono firewall/antivirus e malware; i pc in dotazione del RPCT e dell'eventuale personale preposto è aggiornato periodicamente con firewall/antivirus/ antimalware; capacità di garantire la continuità operativa del sistema (business continuity e disaster recovery), sia da parte dell'Ente che del fornitore e dei soggetti da questo individuati; formazione continua del personale sul tema.	BASSO	1	4	ADEGUATO

	accesso al sistema da parte di personale interno non autorizzato	mancata o errata gestione degli accessi logici da parte del personale - inadeguata configurazione del controllo degli accessi logici ai sistemi - carenza di formazione del personale		adozione di procedure di accesso con credenziali personalizzate; vietato riutilizzo di vecchie password; il sistema utilizzato implementa un protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238; attivazione di procedure di controllo degli accessi logici ai sistemi, nel rispetto della normativa in materia di tutela dei lavoratori (L. 300/1970); sensibilizzazione del personale sul corretto utilizzo delle credenziali.	BASSO	2	2	ADEGUATO
	malfunzionamento software/ piattaforma utilizzata	mancato aggiornamento e manutenzione	D	la piattaforma utilizzata è sottoposta, da parte del fornitore, a manutenzione periodica correttiva, evolutiva con finalità di miglioria continua in materia di sicurezza. L'applicativo GlobalLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza.	BASSO	2	2	ADEGUATO
	malfunzionamento/ mancata sicurezza hardware	carenza di manutenzione periodica dell'hardware/ carenza procedura per risoluzione problemi	D	manutenzione periodica; procedura per tempestiva risoluzione di problemi.	MEDIO	3	2	ADEGUATO
	interruzione continuità operativa dei sistemi ICT	assenza di piani di disaster recovery e business continuity	D	adozione di un sistema di gestione della continuità operativa.	BASSO	2	2	ADEGUATO
	intercettazione di dati e informazioni	linee di comunicazione/traffico di informazioni non protette	R	criptazione dei dati e utilizzo protocolli di sicurezza. L'applicativo GlobaLeaks implementa uno specifico protocollo crittografico realizzato per	BASSO	2	2	ADEGUATO

				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.				
MINACCE RELATIVE AL CONTESTO	accessi non autorizzati a locali/uffici ad accesso riservato - soggetti esterni	mancato o insufficiente controllo degli accessi ai locali (es. accesso libero e non su appuntamento), mancanza sistema di allarme/antintrusione/ scorretta custodia chiavi di accesso/badge	R	accesso ai locali solo su appuntamento; portineria che accoglie gli utenti e li indirizza presso gli uffici; sensibilizzazione del personale su corretta gestione/custodia delle chiavi di accesso/badge; sensibilizzazione del personale su corretta conservazione pratiche.	BASSO	2	2	ADEGUATO

	accessi non autorizzati a locali/uffici ad accesso riservato - soggetti interni	mancanza di misure di sicurezza fisiche per regolazione degli accessi (es. porte non chiuse a chiave); mancata formazione/sensibilizzazione del personale	R	porte degli uffici dotate di serratura e chiuse a chiave quando il personale preposto non è presente; badge/chiavi di accesso agli uffici solo per il personale autorizzato; sensibilizzazione del personale su corretta conservazione pratiche (cassetti/armadi chiusi a chiave).	BASSO	2	2	ADEGUATO
	perdita dati a seguito allagamento/incendio non dovuti a eventi naturali	scarsa manutenzione impianti (idraulico/di raffreddamento/elettrico); mancanza piani di emergenza; mancanza copie di sicurezza	D, I	manutenzione periodica impianti; adozione piani di emergenza per incendio/allagamento; copie di sicurezza dei dati;	BASSO	2	2	ADEGUATO
	perdita di dati a seguito di fenomeni distruttivi naturali (allagamento, incendio, terremoto..)	assenza piani di emergenza, mancanza copie di sicurezza	D, I	sede dell'ente ubicata in zona non sismica/non vicina a corso d'acqua; copie di sicurezza periodiche.	BASSO	2	2	ADEGUATO
	mancanza di alimentazione elettrica/interruzione sistemi	scarsa manutenzione impianto elettrico, sensibilità alla variazione di tensione		installazione gruppo di continuità/ stabilizzazione; manutenzione periodica impianto elettrico.	BASSO	2	2	ADEGUATO

6. Conclusioni

Alla luce della valutazione dei rischi per le libertà e i diritti degli interessati, considerando le contromisure tecniche e organizzative adottate dall'ente sia in materia di Sicurezza delle Informazioni e di Protezione dei dati, nonché le misure di sicurezza adottate dal fornitore della piattaforma utilizzata, la DPIA ha esito POSITIVO, in quanto i rischi risultano di livello MEDIO – BASSO e l'Ente ha implementato misure di sicurezza tali da mitigarlo.

PIANDO D’AZIONE - A fronte dei rischi residui individuati, per il trattamento oggetto della DPIA l’Ente intende migliorare il proprio grado di tutela e sicurezza dei dati personali adottando le seguenti misure:

- adozione di un Regolamento interno /istruzioni su utilizzo credenziali;
- istruzione/ sensibilizzazione del personale sulla corretta conservazione delle credenziali;
- adozione di un Regolamento interno contenente istruzioni/norme comportamentali per i trattamenti verbali di dati;
- formazione/ sensibilizzazione del personale;
- consegna al personale di specifici atti autorizzativi contenenti istruzioni sulle modalità di trattamento
- policy interna / Regolamento interno /istruzioni su gestione delle postazioni di lavoro;
- disattivazione schermata dopo inutilizzo/password di accesso al pc/disconnessione automatica dopo pochi minuti;
- policy interna / Regolamento interno /istruzioni su gestione dei dati in smartworking;
- utilizzo dispositivi personali ma con account specifico per l'attività lavorativa e adeguatamente protetto;
- no utilizzo dispositivi condivisi con familiari;
- sensibilizzazione del personale sul divieto di utilizzare dispositivi removibili personali, sulla corretta custodia degli strumenti e sulla gestione delle stampe;
- backup remoto giornaliero con policy di data retention di 7 giorni;
- i computer del fornitore responsabile del trattamento e dei sub responsabili eseguono firewall/antivirus e malware;
- i pc in dotazione del RPCT e dell'eventuale personale preposto è aggiornato periodicamente con firewall/antivirus/ antimalware;
- capacità di garantire la continuità operativa del sistema (business continuity e disaster recovery), sia da parte dell'Ente che del fornitore e dei soggetti da questo individuati;
- adozione di procedure di accesso con credenziali personalizzate;
- vietato riutilizzo di vecchie password;
- il sistema utilizzato implementa un protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238;
- attivazione di procedure di controllo degli accessi logici ai sistemi, nel rispetto della normativa in materia di tutela dei lavoratori (L. 300/1970);
- la piattaforma utilizzata è sottoposta, da parte del fornitore, a manutenzione periodica correttiva, evolutiva con finalità di miglioria continua in materia di sicurezza. L'applicativo GlobalLeaks e la relativa metodologia di fornitura SaaS sono periodicamente soggetti ad audit di sicurezza.

- manutenzione periodica;
- procedura per tempestiva risoluzione di problemi;
- adozione di un sistema di gestione della continuità operativa;
- criptazione dei dati e utilizzo protocolli di sicurezza.

  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.
- accesso ai locali solo su appuntamento;
- portineria che accoglie gli utenti e li indirizza presso gli uffici;
- sensibilizzazione del personale su corretta gestione/custodia delle chiavi di accesso/badge;
- porte degli uffici dotate di serratura e chiuse a chiave quando il personale preposto non è presente;
- badge/chiavi di accesso agli uffici solo per il personale autorizzato;
- sensibilizzazione del personale su corretta conservazione pratiche (cassetti/armadi chiusi a chiave).
- manutenzione periodica impianti;
- adozione piani di emergenza per incendio/allagamento;
- copie di sicurezza dei dati;
- sede dell'ente ubicata in zona non sismica/non vicina a corso d'acqua;
- copie di sicurezza periodiche.
- installazione gruppo di continuità/ stabilizzazione;
- manutenzione periodica impianto elettrico.

7. Parere del DPO

Il trattamento di dati personali posto in essere dal Comune di Corato nell'esecuzione dei propri compiti di interesse pubblico o comunque connessi all'esercizio dei propri pubblici poteri, con particolare riferimento al compito di accertare eventuali illeciti denunciati nell'interesse dell'integrità dell'Ente, ai sensi di quanto disposto dal D.Lgs. n. 24 del 10 Marzo 2023, dai soggetti che in ragione del proprio rapporto con il Comune vengano a conoscenza di condotte illecite, appare adeguato a quanto previsto dalla normativa sulla protezione dei dati personali (Reg.EU 2016/679).

Il Titolare del Trattamento ha implementato una soluzione organizzativa che prevede l'utilizzoo di nuove tecnologie software che, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. Il Titolare ha correttamente effettuato la valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. La valutazione d'impatto è sufficientemente strutturata, e prende in considerazione i probabili rischi, che sono valutati ed adeguatamente mitigati dalle soluzioni adottate. In particolare, conseguentemente ad una attenta analisi del presente documento, visto l'art. 39 par. 1 lett. C del Reg. 679/2016, il DPO ritiene che i rischi per i diritti e le libertà degli interessati, a seguito dell'adozione delle misure di mitigazione del rischio definite dal Comune di Corato, possano essere qualificati come rischi accettabili in relazione alle finalità perseguite dal trattamento in oggetto.

Il sistema nel suo complesso coniuga in un ragionevole equilibrio il diritto alla riservatezza e protezione dei dati personali dei soggetti interessati con le attività di gestione dei trattamenti connessi al 'whistleblowing', come da disposizioni normative.

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

Richiesta del parere degli interessati

Non è stato richiesto il parere di interessati esterni poichè la predisposizione del canale interno per le segnalazioni è un obbligo di legge (d. lgs. n. 24 del 2023) a cui la PA non può sottrarsi.

Bari, 22/12/23

Il DPO