CITTA' DI MASSAFRA

PROVINCIA DI TARANTO

DELIBERAZIONE DELLA GIUNTA COMUNALE
N. 222 DEL 20/07/2023

OGGETTO: Approvazione valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 13 comma 6 del D. Lgs. n. 24/2023, sul sistema di segnalazione ileciti "WhistleblowingPA"

L'anno duemilaventitre addì venti del mese di Luglio alle ore 12:00, presso la SEDE DELLA GIUNTA, previo esaurimento delle formalità prescritte , si è riunita la Giunta Comunale sotto la presidenza del Sindaco Avv. QUARTO FABRIZIO.

All'appello nominale risulta:

CARICA	COGNOME E NOME	PRESENTE
SINDACO	QUARTO FABRIZIO	SI
VICE SINDACO	LASIGNA DOMENICO	SI
ASSESSORE	CARDILLO IDA	SI
ASSESSORE	PUTIGNANO DOMENICO	SI
ASSESSORE	GUGLIELMI MARIA ROSARIA	--
ASSESSORE	TERMITE ROSA	SI
ASSESSORE	D'ERRICO ANTONIO	SI
ASSESSORE	BRAMANTE MICHELE	SI

Presenti n° 7 Assenti n° 1

Partecipa il Segretario Generale Dott.ssa PERRONE FRANCESCA, il quale provvede alla redazione del presente verbale.

Essendo legale il numero degli intervenuti, l' Avv. QUARTO FABRIZIO, nella sua qualità di Sindaco, assume la presidenza e dichiara aperta la seduta per la trattazione dell'oggetto sopra riportato.

IL SEGRETARIO GENERALE

Premesso che:

- il Comune di Massafra, con l'approvazione del Piano Triennale di Prevenzione della Corruzione e Trasparenza 2019-2021 (PTPCT 2019-2021), in adempimento a quanto previsto dalla normativa nazionale, ha attivato il sistema di segnalazione illeciti, utilizzando la piattaforma sviluppata da Transparency International Italia e dal Centro Hermes per la Trasparenza e i Diritti Umani Digitali, denominata "WhistleblowingPA";
- la piattaforma informatica WhistleblowingPA, è realizzata tramite il software GlobalLeaks ed è conforme alla legge sulla tutela dei segnalanti;
- garantisce il mantenimento e l'aggiornamento della piattaforma e non richiede interventi tecnici da parte di soggetti interni o esterni all'ente;
- è un servizio qualificato DALL'Agenzia per la Cybersicurezza Nazionale (ACN) subentrata, dal 19.01.2023 all'Agenzia per l'Italia Digitale (AGID);

Visto il D. lgs. n. 24 del 10.03.2023 "*Attuazione della direttiva (UE) 2019/1937 del Parlamento Europeo e del Consiglio, del 23 ottobre 2019, riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali";*

Visto, in particolare l'art. 13 comma 6 che dispone: che dispone: "*I soggetti di cui all'articolo 4 definiscono il proprio modello di ricevimento e gestione delle segnalazioni interne, individuando misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato agli specifici rischi derivanti dai trattamenti effettuati, sulla base di una valutazione di impatto sulla protezione dei dati, e disciplinando il rapporto con eventuali fornitori esterni che trattano dati personali per loro conto ai sensi dell'articolo 28 del Regolamento (UE) 2016/679 o dell'articolo 18 del Decreto Legislativo n. 51 del 2018";*

Visto, in particolare, l'art. 24 comma 1 che dispone: "*le disposizioni di cui al presente decreto hanno effetto a decorrere dal 15 luglio 2023";*

Rilevato che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale e che l'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

Considerato che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche, tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

Tenuto presente che tale evoluzione ha indotto l'Unione europea ad adottare il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo "GDPR");

Dato atto che il 24 maggio 2016 è entrato ufficialmente in vigore il GDPR, il quale è diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

Rilevato che, con il GDPR, è stato richiesto agli Stati membri:

- un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

Visto il D. lgs 196/2003, modificato dal D.lgs. 10 agosto 2018 n. 101;

Dato atto che, quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate (a causa del monitoraggio sistematico dei loro comportamenti, o per il gran numero dei soggetti interessati di cui sono magari trattati dati sensibili, o anche per una combinazione di questi e altri fattori), il GDPR obbliga i titolari a svolgere:

- una “determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
- una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Tenuto presente che la DPIA è una procedura prevista dall’art. 35 del Regolamento UE 2016/679 (RGDP) che mira a descrivere un trattamento di dati per valutarne la necessità e la proporzionalità nonché i relativi rischi, allo scopo di approntare misure idonee ad affrontarli;

Tenuto presente l’obbligo, in capo ai titolari, di consultare l’Autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l’impatto del trattamento non siano sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato;

Rilevato che la DPIA deve essere condotta prima di procedere al trattamento e che, deve comunque essere previsto un riesame continuo della DPIA, ripetendo la valutazione a intervalli regolari;

Dato atto che la responsabilità della DPIA spetta al titolare, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all’organizzazione;

Tenuto presente che, ferma restando la discrezionalità dell'amministrazione nell'effettuare la determinazione preliminare e la valutazione di impatto, il Garante, con provvedimento n. 467 dell'11 ottobre 2018, ha reso pubblico l'Elenco delle tipologie di trattamenti da sottoporre obbligatoriamente a valutazione d’impatto, tra cui si menzionano:

1. Trattamenti valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad “aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato”;

2. Trattamenti automatizzati finalizzati ad assumere decisioni che producono “effetti giuridici” oppure che incidono “in modo analogo significativamente” sull’interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. screening dei clienti di una banca attraverso l’utilizzo di dati registrati in una centrale rischi).

3. Trattamenti che prevedono un utilizzo sistematico di dati per l’osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche on-line o attraverso app, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell’informazione inclusi servizi web, tv interattiva, ecc. rispetto alle abitudini d’uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, di previsioni di budget, di upgrade tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.;

4. Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5. Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).

6. Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).

7. Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi wearable; tracciamenti di prossimità come ad es. il wi-fi tracking) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.

8. Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.

9. Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);

10. Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.

11. Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

12. Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

Tenuto presente che, ai sensi dell'art. 29 delle linee guida elaborate dal Gruppo di Lavoro 29 per la protezione dei dati, la DPIA, non è necessaria per i trattamenti che:

- non presentano rischio elevato per diritti e libertà delle persone fisiche
- hanno natura, ambito, contesto, e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni non hanno subito modifiche
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA
- fanno riferimento a norme e regolamenti per la cui definizione è stata condotta una DPIA

Rilevato che, per quanto sopra, è necessario istituire:

1. una "Determinazione preliminare della possibilità che il trattamento possa presentare un rischio elevato" in base alla quale stabilire se un trattamento può, anche solo teoricamente, presentare un rischio elevato;
2. una valutazione di impatto nel caso in cui la determinazione preliminare restituisca l'accertamento della teorica possibilità che il trattamento possa presentare un rischio elevato;

Dato atto che il Comune di Massafra, al fine di garantire la massima diffusione interna ed esterna e la massima conoscibilità dei trattamenti oggetto di DPIA, nonché delle misure tecniche e organizzative individuate dai titolari per mitigare l'impatto del trattamento, è tenuto a garantire la

conoscibilità della Valutazione d'impatto sulla protezione dei dati (DPIA) a tutti i dipendenti dell'Ente;

Dato atto che il procedimento di adozione e approvazione della Valutazione d'impatto sulla protezione dei dati (DPIA) e il presente provvedimento, risultano compatibili con le disposizioni e misure generali previste dal PIAO 2023-2025 e che saranno assunte le misure necessarie in tema di trasparenza e conoscibilità;

PROPONE

per le ragioni indicate in narrativa, e che qui si intendono integralmente richiamate:

1. di approvare, per quanto attiene la Piattaforma in utilizzo presso questo Comune per il sistema di segnalazione illeciti, denominato WhistleblowingPA, la Valutazione d'impatto (DPIA) sulla protezione dei dati (DPIA) ai sensi dell'art. 13 comma 6 del D. Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

2. Di disporre che al presente provvedimento venga assicurata:

a) la pubblicità legale con pubblicazione all'Albo Pretorio;

nonché

b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione "Amministrazione trasparente", sezione di primo livello "Disposizioni generali" sezione di secondo livello "Atti generali";

3. Di dare atto che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell'art. 5 comma 2 D.lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.

4. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

LA GIUNTA COMUNALE

Acquisita la Relazione istruttoria del Segretario Generale e fatta propria;

Visti:

- il D. Lgs. n. 24/2023;
- D.Lgs. 267/2000;
- Legge 241/1990;
- D.Lgs. 196/2003;
- Legge 190/2012;
- D.Lgs. 33/2013;
- Regolamento (UE) n. 679/2016;
- Dichiarazioni del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN;
- Linee-guida sui responsabili della protezione dei dati (RPD) - WP243 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida sul diritto alla "portabilità dei dati" - WP242 Adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- Linee-guida per l'individuazione dell'autorità di controllo capofila in rapporto a uno specifico titolare o responsabile del trattamento - WP244 adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento “possa presentare un rischio elevato” ai sensi del regolamento 2016/679 - WP248 adottate dal Gruppo di lavoro Art. 29 il 4 aprile 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di applicazione e definizione delle sanzioni amministrative - WP253 adottate dal Gruppo di lavoro Art. 29 il 3 ottobre 2017;
- Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali automatizzati e pro lazione - WP251 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Linee guida elaborate dal Gruppo Art. 29 in materia di notifica delle violazioni di dati personali (data breach notification) - WP250 Adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- Parere del WP29 sulla limitazione della finalità - 13/EN WP 203;
- Statuto Comunale;
- Regolamento di organizzazione degli uffici e dei servizi;
- Regolamento sul trattamento dei dati sensibili;
- Codice di comportamento del Comune di Massafra;
- Circolari e direttive del RPC;

Visto il parere in ordine alla regolarità tecnica ai sensi dell’art. 49 comma 1 del D. Lgs. n. 267/2000;

Ritenuto di provvedere in merito;

A votazione unanime e palese

DELIBERA

1. di approvare, per quanto attiene la Piattaforma in utilizzo presso questo Comune per il sistema di segnalazione illeciti, denominato WhistleblowingPA, la Valutazione d’impatto (DPIA) sulla protezione dei dati (DPIA) ai sensi dell’art. 13 comma 6 del D. Lgs. n. 24/2023, allegata alla presente, per formarne parte integrante e sostanziale;

2. Di disporre che al presente provvedimento venga assicurata:

a) la pubblicità legale con pubblicazione all’Albo Pretorio;

nonché

b) la trasparenza mediante la pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione “Amministrazione trasparente”, sezione di primo livello “Disposizioni generali" sezione di secondo livello “Atti generali”;

3. Di dare atto che, in disparte la pubblicazione sopra indicata, chiunque ha diritto, ai sensi dell’art. 5 comma 2 D.lgs. 33/2013 di accedere ai dati e ai documenti ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del citato D.lgs. 33/2013, nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti secondo quanto previsto dall'articolo 5-bis del medesimo decreto.

4. Di disporre che la pubblicazione dei dati, delle informazioni e dei documenti avvengano nella piena osservanza delle disposizioni previste dal D.lgs. 196/2003 e, in particolare, nell'osservanza di quanto previsto dall'articolo 19, comma 2 nonché dei principi di pertinenza, e non eccessività dei dati pubblicati e del tempo della pubblicazione rispetto ai fini perseguiti.

Infine, la Giunta Comunale, stante l’urgenza di provvedere, con separata ed unanime votazione

DELIBERA

5. di dichiarare il presente provvedimento immediatamente eseguibile, ai sensi dell'articolo 134, comma 4 del D. Lgs. n. 267/2000, in ragione dell'esigenza di celerità correlata alla protezione dei dati e alla efficienza dei procedimenti amministrativi.

PARERE DI REGOLARITA' TECNICA

Ai sensi dell'art. 49 c.1 del T.U.E.L. il Dirigente **PERRONE FRANCESCA** in data **20/07/2023** ha espresso parere **FAVOREVOLE**,
Dott.ssa PERRONE FRANCESCA

LETTO APPROVATO E SOTTOSCRITTO

Il Sindaco	**Il Segretario Generale**
Avv. QUARTO FABRIZIO	**Dott.ssa PERRONE FRANCESCA**

NOTA DI PUBBLICAZIONE N. 2672

Ai sensi dell'art. 124 del T.U. 267/2000 il Responsabile della Pubblicazione **GALLO SABINO** attesta che in data 20/07/2023 si è proceduto alla pubblicazione sull'Albo Pretorio.

La Delibera è esecutiva ai sensi ex art. 134, comma 4 del T.U.E.L..

Massafra, lì 20/07/2023

Il Firmatario della pubblicazione

GALLO SABINO

C I T T A ’ D I M A S S A F R A

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

DATA PROTECTION IMPACT ASSESSMENT

VALUTAZIONE DI IMPATTO
PROTEZIONE DATI RIGUARDANTI I SOGGETTI CHE SEGNALANO VIOLAZIONI DELLE DISPOSIZIONI NORMATIVE NAZIONALI

(Ex art. 13 Comma 6 d. Lgs. N. 24/2023)

C I T T A ’ D I M A S S A F R A

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

SOMMARIO

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

1. PREMESSA

Con l'approvazione del PTPCT 2019-2021 il Comune di Massafra, in adempimento a quanto previsto dalla normativa nazionale, ha attivato il sistema di segnalazione illeciti.

La piattaforma in utilizzo è stata sviluppata da Transparency International Italia e dal Centro Hermes per la Trasparenza e i Diritti Umani Digitali.

Essa è raggiungibile al seguente link, il cui logo è pubblicato sulla home page del Comune di Massafra e sul sito Amministrazione Trasparente nella apposita sezione.

https://comunedimassafra.whistleblowing.it/#/

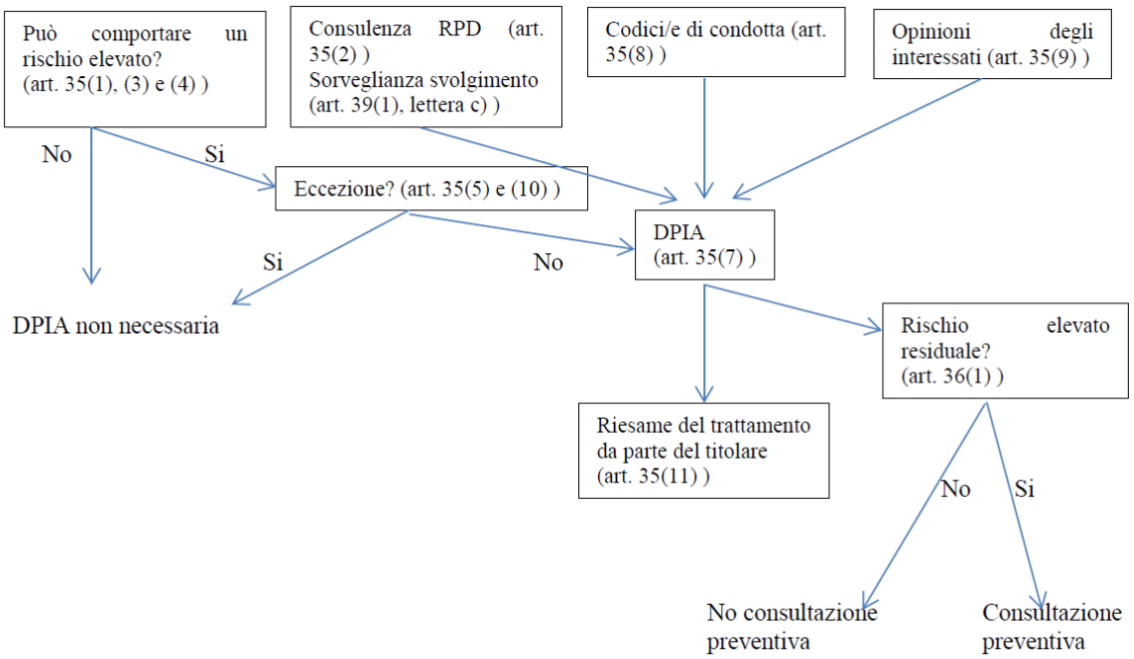
In attuazione di quanto previsto dall'art. 13 comma 6 del D. Lgs. n. 24/2023 e dall'art. 35 del GDPR n. 679/2016, si redige apposita Valutazione di impatto per come di seguito meglio specificato, predisposta da Whistleblowing Solutions e fatta propria, personalizzandola, per le proprie specifiche, dal Comune di Massafra.

La Valutazione d'Impatto sulla Protezione dei Dati (di seguito "DPIA\ è un processo che il Titolare del trattamento deve effettuare, in via preventiva, ogni qual volta un trattamento di dati personali, in particolare connesso all'impiego di nuove tecnologie, in considerazione della natura, dell'oggetto, del contesto e delle finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà delle persone.

Il processo di DPIA è ritenuto uno degli aspetti di maggiore rilevanza nel nuovo quadro normativo definito dal Regolamento Generale sulla Protezione dei Dati (Regolamento UE 2016/679), in quanto esprime chiaramente la responsabilizzazione (c.d. accountability) del titolare nei confronti dei trattamenti dallo stesso effettuati.

Il Titolare del trattamento, infatti, è tenuto non solo a garantire l'osservanza delle disposizioni regolamentari, quanto anche a dimostrare adeguatamente in che modo egli garantisca tale osservanza.

Whistleblowing Solutions, nel suo ruolo di Responsabile, per il Comune di Massafra, del trattamento per la gestione del sistema di whistleblowing, con il presente documento intende fornire tutti gli elementi ai Titolari per svolgere la valutazione di impatto così come previsto dall'art. 35 del Regolamento.



Principi fondanti il processo di DPIA

2. DESCRIZIONE DELLA PIATTAFORMA DI WHISTLEBLOWING

Whistleblowing Solutions, in qualità di responsabile del trattamento, si occupa della gestione del sistema di whistleblowing 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.
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

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

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.

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

3. DESCRIZIONE E ANALISI DEL CONTESTO

Responsabilità connesse al trattamento:	**PA, Ente o Organizzazione** > Comune di Massafra **Whistleblowing Solutions** > Responsabile del trattamento per la fornitura e la gestione del sistema di whistleblowing **Seeweb** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la gestione dell'infrastruttura \IaaS\ **Transaparency International Italia** > Sub-Responsabile del trattamento, nominato da Whistleblowing Solutions, per la collaborazione nella gestione del sistema di whistleblowing
Standard applicabili:	**Conformità normativa:** • 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 • Certificazione CSA Star
Dati e operazioni di trattamento:	Operazioni informatizzate di trattamento di dati personali relative alla raccolta e conservazione dei dati necessari per l'erogazione dei servizi in modalità SaaS così come pattuito tra le parti. **Dati di registrazione** Dati identificativi e di contatto dei referenti del Titolare che attivano il servizio di digital whistleblowing (es. Responsabile Anticorruzione). **Categorie particolari di dati** Dati eventualmente contenuti nelle segnalazioni e in atti e documenti ad essa allegati. **Dati relativi a condanne penali e reati** Dati eventualmente contenuti nella segnalazione e in atti e documenti ad essa allegati.
Ciclo di vita del trattamento e dei dati	1\ Attivazione della piattaforma 2\ Configurazione della piattaforma 3\ Fase d'uso della piattaforma con caricamento delle segnalazioni da parte dei segnalanti e accesso alle stesse

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

	da parte dei riceventi preposti 4\ Fase di dismissione della piattaforma al termine del contratto e alla scadenza degli obblighi di legge per

	finalità amministrative e contabili con conseguente cancellazione sicura dei dati da parte del fornitore
Risorse a supporto delle attività di trattamento:	Software di whistleblowing professionale GlobaLeaks Infrastruttura IaaS e SaaS privata basata su tecnologie: - Dettaglio Hardware - VMWARE (virtualizzazione) - Debian Linux LTS (sistema operativo) - VEEAM (backup) - OPNSENSE (firewall) - OPENVPN (vpn)

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

4. VALUTAZIONI IN MERITO AI TRATTAMENTI

PRINCIPI FONDAMENTALI

Adeguatezza, pertinenza e limitazione a quanto è necessario in relazione alle finalità per le quali i dati sono trattati (minimizzazione)	Per la registrazione e attivazione del servizio sono richiesti unicamente i seguenti dati: Nome, Cognome, Ruolo, Telefono, Email di ruolo dell'utente che effettua la registrazione e i dati relativi all'ente (nome, indirizzo, CF e PI\. Il software di whistleblowing raccoglie segnalazioni secondo i migliori questionari predisposti in ambito di whistleblowing in collaborazione con importanti enti di ricerca in materia di whistleblowing e anticorruzione e messi a punto da Transparency International Italia in relazione alla normativa vigente in materia. Nel rispetto del principio di privacy by design tutti i dispositivi utilizzati quali applicativo GlobaLeaks, log di sistema e firewall sono configurati per non registrare alcun tipo di log di informazioni lesive della privacy e dell'anonimato del segnalante quali per esempio indirizzi IP, User Agents e altri Metadata. L'applicativo GlobaLeaks vede abilitata la possibilità di navigazione tramite Tor Browser per finalità accesso anonimo con garanzie al passo con lo stato dell'arte della ricerca tecnologica in materia.

Esattezza e aggiornamento dei dati	L'aggiornamento dei dati è a cura degli utenti stessi che si sono registrati attraverso l'accesso alla propria area riservata. Non appena vengono modificati i dati di contatto all'interno della piattaforma, questi diventano i dati di contatto ufficiali a cui sono inviate le comunicazioni relative a ogni tipo di aggiornamento.

Periodo di conservazione dei dati	Policy di data retention di default delle segnalazioni di 18 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.

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

Definizione degli obblighi dei responsabili del trattamento e	Gli accordi contrattuali sono definiti con le seguenti società

formalizzazione dei contratti	• 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

Protezione in caso di trasferimento di dati al di fuori dell'Unione europea:	I Dati Personali sono trattati principalmente in Italia ed esclusivamente nei Paesi dell'Unione Europea. Non esiste alcun trasferimento di Dati Personali verso l'estero in paesi extra UE.

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

5. MISURE DI SICUREZZA

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

CONTROLLO DEGLI ACCESSI LOGICI

L'accesso applicativo è consentito ad ogni utilizzatore autorizzato tramite credenziali di autenticazione personali.

Il sistema implementa policy password sicura e vieta il riutilizzo di precedenti password.

Il sistema implementa protocollo di autenticazione a due fattori con protocollo TOTP secondo standard RFC 6238.

Gli accessi privilegiati alle risorse amministrative sono protetti tramite accesso mediato via VPN.

TRACCIABILITÀ

L'applicativo GlobaLeaks implementa un sistema di audit log sicuro e privacy preserving atto a registrare le attività effettuate dagli utenti e dal sistema in compatibilità con la massima confidenzialità richiesta dal processo di whistleblowing.

I log delle attività del segnalante sono privi delle informazioni identificative dei segnalanti quali indirizzi IP e User Agent.

I log degli accessi degli amministratori di sistema vengono registrati tramite moduli syslog e registri remoti centralizzati.

C I T T A ’ D I M A S S A F R A

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

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.

GESTIONE DELLE VULNERABILITÀ TECNICHE

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

BACKUP

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

MANUTENZIONE

E' prevista manutenzione periodica correttiva, evolutiva e con finalità di miglioria continua in materia di sicurezza.

Per i server applicativi virtuali che realizzano il servizio di whistleblowing è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

Per i sistemi che compongono l'infrastruttura fisica, di backup e firewall è prevista una modalità di manutenzione accessibile al solo personale Whistleblowing Solutions e del relativo fornitore SaaS attraverso cui svolgere le modifiche al sistema installare gli aggiornamenti previsti.

SICUREZZA 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.

SICUREZZA DELL'HARDWARE

I datacenter del fornitore IaaS dispongono di un'infrastruttura dotata di controllo degli accessi, procedure di monitoraggio 7x24 e videosorveglianza tramite telecamere a circuito chiuso, in aggiunta al sistema di allarme e barriere fisiche presidiate 7x24.

I datacenter del fornitore IaaS sono certificati ISO27001.

C I T T A ’ D I M A S S A F R A

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

GESTIRE GLI INCIDENTI DI SICUREZZA E LE VIOLAZIONI DEI DATI PERSONALI

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

CITTA' DI MASSAFRA

Provincia Di Taranto
Municipio Via Livatino s.n.c.
74016 Massafra

LOTTA CONTRO IL MALWARE

Tutti i computer del personale di Whistleblowing e dei sub-responsabili nominati eseguono firewall e antivirus come da policy aziendale ed il personale riceve continua e aggiornata formazione al passo con lo stato dell'arte in materia di lotta contro il malware.
Parimenti le utenze del servizio di whistleblowing vengono sensibilizzate sulla tematica tramite formazione diretta o documentazione online.

6. 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