COMUNE DI ORIO LITTA

Provincia di Lodi

Decreto numero 2 del 18-09-2023

OGGETTO:	**APPROVAZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA) AI SENSI DEL REGOLAMENTO (UE) N. 679/2016 RELATIVA AL TRATTAMENTO DATI CONCERNENTE IL WHISTLEBLOWING ATTUATO MEDIANTE LA PIATTAFORMA TELEMATICA DI TRASPARENCY INTERNATIONAL ITALIA**

IL SINDACO

RICHIAMATI:

- la Legge 6 novembre 2012 n. 190 *"Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione*;
- la Legge 30 novembre 2017 n. 179 *"Disposizioni per la tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro pubblico o privato"*;
- l'art. 54-bis del Decreto Legislativo 30 marzo 2001 n. 165 *"Tutela del dipendente pubblico che segnala illeciti";*

VISTA la 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;

VISTO il Decreto Legislativo 10 marzo 2023 n. 24 recante *"Attuazione della direttiva (UE) 2019/1937 del Parlamento europeo e del Consiglio del 23 ottobre 2019 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione e recante disposizioni riguardanti la protezione delle persone che segnalano violazioni delle disposizioni normative nazionali (Decreto whistleblowing)";*

RICHIAMATO, in particolare, l'art. 4, comma 1, del D.Lgs. n. 24/2023 il quale stabilisce che *"i soggetti del settore pubblico e i soggetti del settore privato, sentite le rappresentanze o le organizzazioni sindacali di cui all'articolo 51 del decreto legislativo n. 81 del 2015, attivano propri canali di segnalazione, che garantiscano, anche tramite il ricorso a strumenti di crittografia, la riservatezza dell'identità della persona segnalante, della persona coinvolta e della persona comunque menzionata nella segnalazione, nonché del contenuto della segnalazione e della relativa documentazione"*;

DATO ATTO che:

- l'Autorità Nazionale Anticorruzione (ANAC), con apposita deliberazione n. 311 del 12/07/2023 ha approvato le nuove "*Linee Guida in materia di protezione delle persone che segnalano violazioni del diritto dell'Unione e delle disposizioni normative nazionali*";
- la materia è stata oggetto dapprima di una riforma introdotta con la Legge 179/2017, quindi è stata ulteriormente innovata, alla luce del recepimento in Italia della Direttiva UE 2019/1937, con il D.Lgs. 24/2023, entrato in vigore il 15/7/2023;

EVIDENZIATO che con le nuove disposizioni l'istituto si applica anche agli operatori che collaborano con le aziende contrattualizzate dal Comune di Orio Litta per concessioni o appalti;

DATO ATTO che la gestione informatizzata delle segnalazioni deve avvenire in maniera del tutto anonima per tutelare l'identità del segnalante e metterlo al riparo da eventuali condotte ritorsive ed

essere gestita dal Responsabile Anticorruzione dell'Ente;

RILEVATO che il Piano integrato di attività e organizzazione (P.I.A.O.) 2023/2025 del Comune di Orio Litta, approvato con deliberazione di Giunta Comunale n. 23 del 07/04/2023 prevede nella sezione 2.3 "Anticorruzione e Trasparenza", alla Misura n. 5, "Adozione di misure per la tutela del dipendente che effettua segnalazioni di illecito (whistleblower)", l'adozione di un "*sistema informatizzato per l'inoltro e la gestione di segnalazioni in maniera del tutto anonima e che ne consente l'archiviazione";*

VISTA la deliberazione della Giunta comunale n. 45 del 28/07/2023 con cui il Comune ha deciso di dotarsi della piattaforma gratuita di Traparency International Italia mediante SOFTWARE GLOBALEAKS per gestire il sistema delle segnalazioni da parte di dipendenti e collaboratori dell'Ente (c.d. whistleblowing) di reati o irregolarità di cui siano venuti a conoscenza in ragione del rapporto di lavoro, ai sensi dell'art. 54 bis del D.Lgs. 165/2001;

VISTO il Decreto sindacale n. 9 del 11/06/2019 con cui il Segretario comunale - Responsabile della Prevenzione della Corruzione e della Trasparenza, Dott.ssa Maria Rosa Schillaci, viene nominata quale persona autorizzata al trattamento di dati personali in relazione al procedimento *Whistleblowing* e contestualmente vengono assegnati i compiti e le funzioni inerenti;

VISTI**:**

- il Regolamento UE 2016/679 "General Data Protection Regulation" (di seguito anche GDPR);
- il D.Lgs.196/2003 "Codice in materia di protezione dei dati personali (di seguito anche Codice), come modificato ed integrato dal D.Lgs.101/2018;

DATO ATTO che:

- il Regolamento UE 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 (c.d. GDPR), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, è applicabile dal 25 maggio 2018 ed è stato recepito in Italia per mezzo del D.Lgs. 101/2018 mediante l'aggiornamento del T.U. sul trattamento dei dati personali (c.d. "Privacy"), D.Lgs. 196/2003;
- l'art. 35 del GDPR prevede che "*quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione (definita valutazione di impatto o DPIA) può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi*". Inoltre, al paragrafo 7 il legislatore europeo stabilisce che la valutazione contenga almeno:
  a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
  b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
  c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1;
  d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione;

RILEVATO che la Valutazione di impatto (DPIA) di cui all'art. 35 del Reg. UE 2016/679 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, nella persona del sindaco pro-tempore, anche se la conduzione materiale della valutazione di impatto può essere affidata ad un altro soggetto, interno o esterno all'organizzazione;

VISTA la Determina n. 249 del 15/12/2022 con cui viene designato quale Responsabile della Protezione Dati personali (RDP o DPO) per il Comune di Orio Litta, ai sensi dell'art. 37 del Regolamento UE 2016/679, la società Galli Data Service srl con sede a Piacenza che, a sua volta, ha individuato quale referente per questo ente l'avvocato Valentina Groppi, nomina resa nota tramite

inserimento del nominativo e degli estremi di contatto sul sito dell'Autorità Garante per la protezione dei dati personali e sul sito istituzionale del Comune;

EVIDENZIATO che il DPO ha predisposto la Valutazione di Impatto (DPIA) relativa al trattamento *Whistleblowing*, trasmessa in data 03/08/2023, che si compone di 12 articoli, allegata quale parte integrante e sostanziale al presente atto;

DATO ATTO che dal documento di Valutazione di Impatto emerge che, tenuto conto dell'analisi dei rischi e delle misure di sicurezza adottate, il rischio residuo legato al trattamento *Whistleblowing* risulta accettabile;

RITENUTO di procedere all'approvazione della Valutazione di Impatto (DPIA) relativa al trattamento dati Whistleblowing del Comune di Orio Litta e alla sua pubblicazione nelle apposite sezioni del sito istituzionale dell'ente,

DECRETA

in merito e per tutto quanto su esposto, fino a diversa determinazione,

1. DI APPROVARE la Valutazione di impatto (DPIA) di cui all'art. 35 del Reg. UE 2016/679 relativa al trattamento dati Whistleblowing da attuare mediante la piattaforma telematica gratuita di Trasparency International Italia tramite SOFTWARE GLOBALEAKS, che gestisce le segnalazioni di reati o irregolarità da parte dei dipendenti e collaboratori del Comune di Orio Litta o da operatori che collaborano con le aziende contrattualizzate dal Comune per concessioni o appalti, predisposta dal DPO e trasmessa in data 03/08/2023, che si compone di 12 articoli, allegata quale parte integrante e sostanziale al presente atto;
- All. "A";

2. DI DARE ATTO che dal documento di Valutazione di Impatto emerge che il DPO – Ditta Galli Data Service, tenuto conto dell'analisi dei rischi e delle misure di sicurezza adottate, ha attestato l'assenza di rischi elevati rispetto al trattamento in parola.

DISPONE

inoltre che copia del presente atto e della Valutazione di Impatto – DPIA:

- sia pubblicata all'Albo Pretorio online e sul sito istituzionale del Comune di Orio Litta, sezione Amministrazione Trasparente, sottosezione *Altri contenuti – Prevenzione della Corruzione* – Whistleblowing;

- sia trasmessa, per quanto di rispettiva competenza, al Segretario comunale, Responsabile della Prevenzione della corruzione e per la Trasparenza (RPCT), al Responsabile del Servizio informatico nonché al Responsabile della Transizione Digitale (RTD) oltre che allo stesso Responsabile Trattamento Dati (DPO).

IL SINDACO
Francesco Ferrari
Firmato digitalmente ex D.Lgs. 82/2005

L'originale del presente atto, dopo la pubblicazione all'Albo Pretorio on line, viene conservato negli archivi informatici dell'Ente.

Valutazione di impatto sulla protezione dei dati

APPROVATO DA:

……

(Timbro/Firma Titolare)

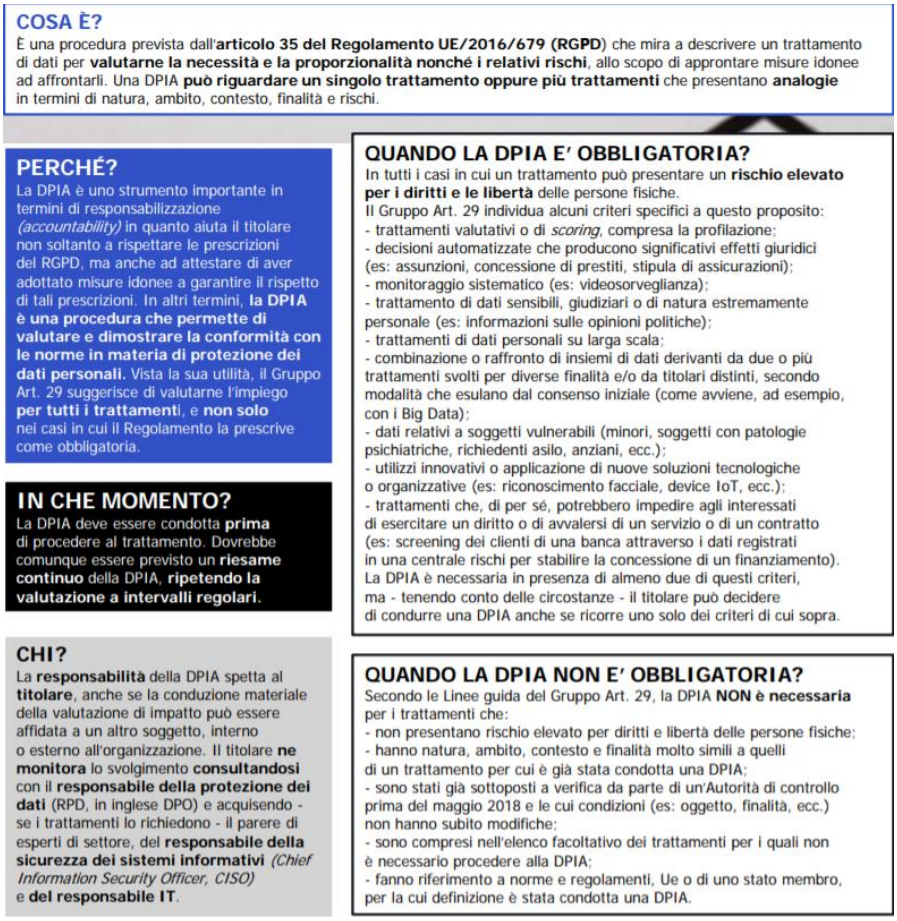
1) Scopo del documento e riferimenti normativi

Il presente documento risponde all'obbligo previsto dall'Art. 13(6) del D.Lgs.24/2023 e viene redatto in conformità all'Art.35 del Reg.UE 2016/679 "Valutazione d'impatto sulla protezione dei dati" (o Privacy Impact Assessment, di seguito anche PIA). Il presente documento contiene inoltre gli elementi di cui all'Art.30 del Reg.UE 2016/679 "Registri delle attività di trattamento". Il presente documento è pertanto da considerarsi come parte integrante di:

- Modello di ricevimento e gestione delle segnalazioni whistleblowing (al quale si rimanda per eventuali approfondimenti);
- Sistema di conformità privacy dell'Ente.

2) Definizione PIA

Una PIA è 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 le misure per affrontarli. Le valutazioni d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono il Titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento. In altre parole, una **valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità del trattamento**. La PIA può riguardare un singolo trattamento o trattamenti multipli simili tra di loro, in termini di natura, ambito di applicazione, contesto, finalità e rischi.
Di seguito l'infografica dell'Autorità Garante per la protezione dei dati riferita alla PIA
https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7185457

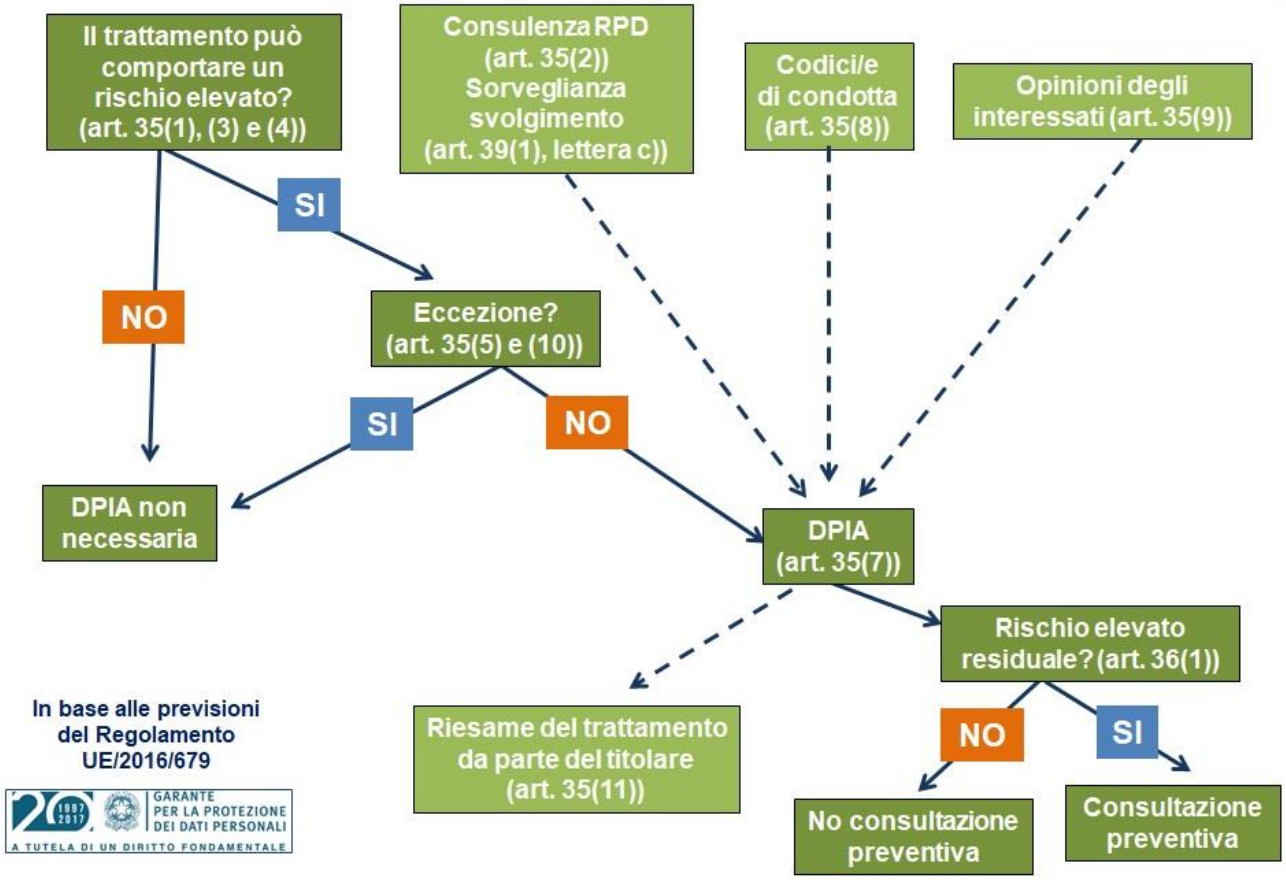


2) Indicazioni legali sulla conduzione della PIA

La conduzione della PIA avviene secondo i seguenti riferimenti normativi:

- GDPR, Art.35 del Regolamento UE 2016/679 “Valutazione d'impatto sulla protezione dei dati”;
- GDPR, Considerando 84, 89-93, 95;
- Gruppo di lavoro Art.29 per la protezione dei dati (WP248 rev.01) “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” adottate il 04/05/2017 e modificate il 04/10/2017;
- Provvedimento dell’Autorità Garante Italiana N°467 del 11/10/2018 “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” pubblicato in Gazzetta Ufficiale N°269 del 19/11/2018;
- Linee guida destinate ai Responsabili della protezione dei dati per il rispetto del Regolamento generale sulla protezione dei dati dell’Unione Europea (versione approvata dalla Commissione, luglio 2019).

Di seguito l’infografica dell’Autorità Garante che presenta lo scenario di conduzione della PIA



3) Quando condurre una PIA

E' necessario condurre una PIA qualora:

- ricorra il criterio generale di rischio elevato previsto dall'Art.35, comma 1;
- ricorra almeno uno dei casi particolari previsti dall'Art.35, comma 3;
- ricorrano 2 o più criteri tra quelli previsti dal WP29;
- un trattamento soggetto al meccanismo di coerenza rientri nelle tipologie previste dall'All.1 del Provv. 467 del 11/10/2018.

Criterio principale La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria qualora il trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4).

Casi particolari La PIA è richiesta in particolare nei casi seguenti:

- una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
- il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10; o
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Criteri previsti da WP29 La PIA è richiesta al ricorrere di 2 o più dei seguenti criteri:

- valutazione o assegnazione di un punteggio, inclusiva di profilazione e previsione, in particolare in considerazione di "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";
- processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente sulle persone;
- monitoraggio sistematico degli interessati;
- dati sensibili o dati aventi carattere altamente personale;
- trattamento di dati su larga scala;
- creazione di corrispondenze o combinazione di insiemi di dati;
- dati relativi a interessati vulnerabili;
- uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative;
- quando il trattamento in sé "impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto".

Criteri previsti dal Garante Italiano In caso di trattamenti soggetti al meccanismo di coerenza, la PIA è richiesta al ricorrere di almeno uno dei seguenti criteri:

- 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"
- 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)
- 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.
- 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).

- 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).
- Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
- 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 WP248, rev. 01 .
- Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
- 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).
- 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.
- Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
- Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento

4) Metodologia di conduzione della PIA

4.1) Tempistica

La PIA va effettuata "**prima del trattamento**", in coerenza con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita. La PIA va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento. La PIA è un **processo continuo**, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

4.2) Soggetti

- Al **Titolare del trattamento** spetta assicurare che la PIA sia eseguita. La PIA può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito.
- Il Titolare deve consultare il **Responsabile della protezione dei dati** ed eventuali **Responsabili del trattamento**.
- E' consigliabile che il Titolare raccolga le opinioni **degli interessati o dei loro rappresentanti**.
- E' consigliabile che fornisca assistenza al Titolare il **capo della sicurezza dei sistemi di informazione (e/o il dipartimento IT).**

4.3) Contenuti

Il GDPR definisce le caratteristiche minime dei contenuti di una PIA, che deve fornire almeno:

- una descrizione dei trattamenti previsti e delle finalità del trattamento;
- una valutazione della necessità e proporzionalità dei trattamenti;
- una valutazione dei rischi per i diritti e le libertà degli interessati;
- le misure previste per affrontare i rischi e dimostrare la conformità al GDPR.

Di seguito l'infografica dell'Autorità Garante che presenta il processo di conduzione della PIA

4.4) Conclusioni

All'esito della PIA il Titolare è tenuto a:

- procedere con il trattamento qualora la PIA indichi che il livello di rischio è correttamente attenuato da adeguate misure di sicurezza, che garantiscano un livello di rischio residuo accettabile;
- procedere con un riesame qualora insorgano variazioni negli elementi analizzati tramite la PIA;
- consultare l'autorità Garante ogni qualvolta non sia in grado di trovare misure sufficienti per ridurre i rischi ad un livello accettabile.

5) La necessità di condurre una PIA in riferimento al Whistleblowing

Indipendentemente dai criteri di cui al Cap.3 "Quando condurre una PIA", nel caso in esame l'obbligo è sancito direttamente dal Legislatore, ai sensi dell'Art.13(6) del D.Lgs.24/2023 "Trattamento dei dati personali": *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 d'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.*

6) Descrizione del trattamento

Tipologia di dati trattati	Sono trattati tutti i dati personali contenuti nel processo di segnalazione, nonché negli eventuali successivi approfondimenti di indagine. Tali dati possono essere qualificati come comuni (dati anagrafici) o relativi a reati (GDPR, Art.10). Di norma, a meno di dati inseriti volontariamente dal segnalante, si esclude il trattamento di dati appartenenti alle categorie particolari (GDPR, Art.9)
Attività di trattamento	In funzione degli obblighi normativi sono possibili i seguenti trattamenti: raccolta, registrazione, conservazione, consultazione, trasmissione, cancellazione
Finalità del trattamento	I dati sono trattati allo scopo di una corretta gestione delle segnalazioni, connessi adempimenti normativi, riscontri al segnalante ed eventuali approfondimenti di indagine.
Base giuridica del trattamento	La base giuridica del trattamento è da rinvenirsi nell'Art.6, comma1(c) "il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il Titolare".
Modalità e strumenti del trattamento	I dati sono trattati secondo modalità e con strumenti atti a garantirne la massima sicurezza e riservatezza. L'identità del segnalante è protetta secondo le prescrizioni di cui all'Art. 12 del D.Lgs.24/2023 "Obbligo di riservatezza". La società ha adottato quale canale di segnalazione interno una piattaforma on-line, dotata dei necessari requisiti di sicurezza
Conservazione dei dati	I dati sono trattati per tempi compatibili con le prescrizioni normative, con specifico riferimento all'Art.14 del D.Lgs.24/2023 "*Conservazione della documentazione inerente alle segnalazioni*": le segnalazioni e la relativa documentazione sono conservate per il tempo necessario al trattamento della segnalazione e comunque **non oltre cinque anni** a decorrere dalla data della comunicazione dell'esito finale della procedura di segnalazione. In caso di inserimento da parte dei segnalanti di dati manifestamente non utili alla gestione della segnalazione, il Gestore procederà all'immediata cancellazione, compatibilmente con i vincoli tecnici della piattaforma
Ambito di conoscibilità	Potranno accedere ai dati esclusivamente soggetti formalmente designati, autorizzati ed istruiti, tra cui: gestore del canale di segnalazione, organi di controllo, ecc. In caso di indagini i dati potranno essere conosciuti dalle pubbliche autorità preposte. In generale i dati potranno essere conosciuti nell'ambito delle prescrizioni di cui all'Art.12 del D.Lgs.24/2023.

7) Aderenza ai principi generali

Liceità	Il trattamento viene effettuato nell'espletamento di un obbligo legale a cui è soggetto il Titolare.
Limitazione della finalità	Si esclude l'utilizzo dei dati per fini differenti rispetto agli adempimenti di legge.
Minimizzazione	La piattaforma è configurata con i campi necessari all'acquisizione dei dati indispensabili alla gestione delle segnalazioni. Il segnalante è tenuto ad inserire informazioni pertinenti (si diffondono dettagliate istruzioni in tal senso).
Esattezza	Il segnalante è tenuto a inserire informazioni di cui abbia ragionevole certezza (si diffondono dettagliate istruzioni in tal senso).
Limitazione della conservazione	Vedi paragrafo precedente
Integrità e riservatezza	Vedi misure di sicurezza

8) Informazioni e diritti degli interessati

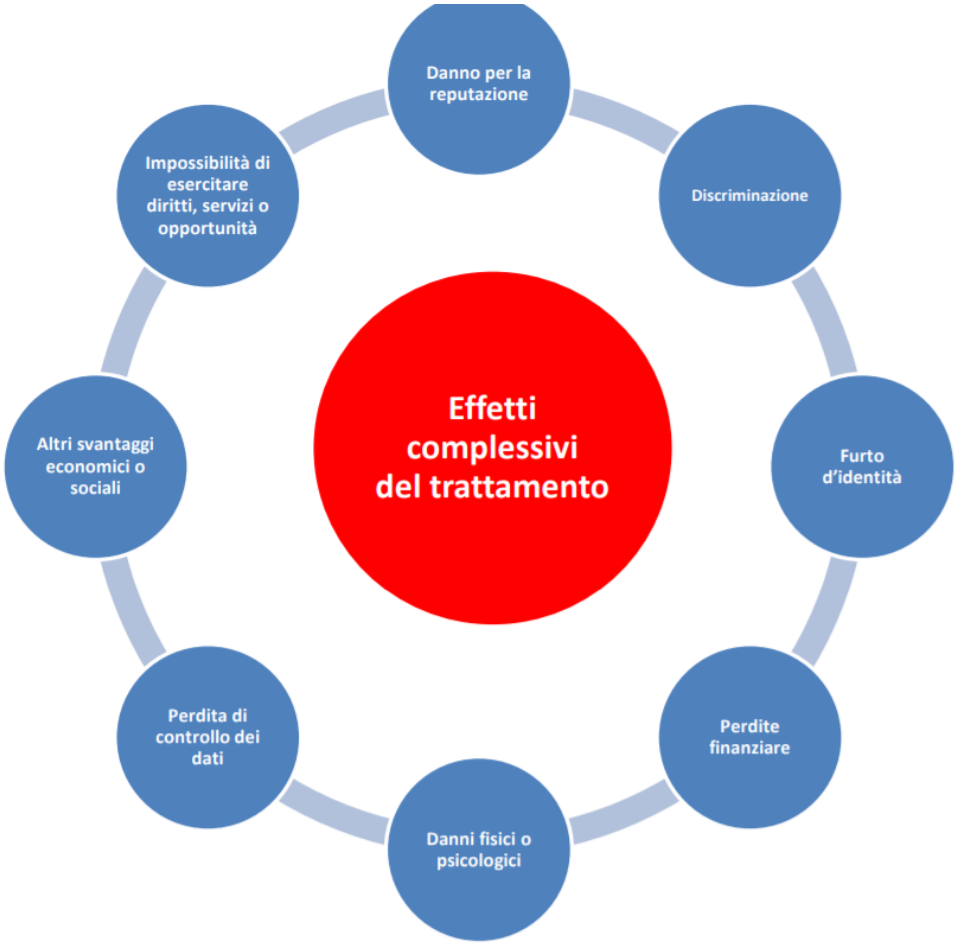
Modalità di diffusione dell'informativa (GDPR, Art.13)	Il Titolare ha adottato adeguati canali di diffusione delle istruzioni in merito a come effettuare una segnalazione: ◎ pubblicazione istruzioni su proprio sito internet ◎ esposizione infografica presso sede ◎ consegna istruzioni ai dipendenti ◎ inserimento disclaimer email Su proprio sito web è inoltre disponibile apposito documento contenente note legali ed informativa privacy riferita al trattamento dei dati contenuti nelle segnalazioni Sul portale di segnalazione sono presenti ulteriori specifiche tecniche sui requisiti di sicurezza della piattaforma
Modalità di garanzia di esercizio dei diritti degli interessati (GDPR, Art.15-21)	Si segnala che i diritti di cui agli articoli da 15 a 22 del GDPR possono essere esercitati nei limiti di quanto previsto dall'articolo 2-undecies del D.Lgs.196/2003 "Limitazioni ai diritti dell'interessato", ossia rivolgendosi direttamente all'Autorità Garante.

9) Valutazione del rischio

Al fine di identificare una corretta metodologia di analisi dei rischi, Il Titolare si base sulle indicazioni dell'Autorità Garante diffuse al seguente link: http://www.garanteprivacy.it/regolamentoue/dpia/gestione-del-rischio

Pertanto, preliminarmente alla definizione della metodologia occorre focalizzare il vero obiettivo dell'analisi di rischio prevista dal GDPR, ossia **l'impatto sui diritti e le libertà fondamentali delle persone fisiche**. Il legislatore focalizza dunque il processo sull'interessato, invitando a sensibilizzare il Titolare sulle possibili conseguenze che i trattamenti effettuati possano generare sulle persone che hanno conferito tali dati

(interessati). In particolare occorre identificare una metodologia che definisca quale livello di rischio per gli interessati possa derivare da un evento dannoso quale distruzione accidentale o illegale, perdita, modifica, rivelazione o accesso non autorizzato in funzione delle possibili conseguenze illustrate nella seguente figura.



La seguente tabella classifica una sintesi dei suddetti elementi in funzione del trattamento in oggetto.

RISCHIO	MINACCIA	PROB.	GRAV.	IMPATTO SUGLI INTERESSATI
Accesso illegittimo	Comportamento fraudolento degli operatori o soggetti esterni	BASSA	MEDIA	Potenziale utilizzo improprio dei dati; danni reputazionali, discriminazione
Modifica indesiderata	Comportamento fraudolento degli operatori o soggetti esterni	BASSA	MEDIA	Potenziale utilizzo improprio dei dati; danni reputazionali, discriminazione
Distruzione, perdita	Eventi distruttivi; errore umano	BASSA	BASSA	

Il sistema non risulta esposto ad eventuali ulteriori impatti negativi per l'interessato quali: danni fisici o fisiologici, furto di identità, perdita di controllo dei dati, ecc.

10) Misure di sicurezza e rischio residuo

Accesso ai dati	• Al fine di limitare il rischio di utilizzo improprio del sistema, il Titolare ha optato per una piattaforma interamente esternalizzata, Whistleblowing PA, basata sul supporto di fornitori qualificati e su strumenti certificati. • Tutti i soggetti che possono accedere ai dati sono regolarmente designati ed istruiti. • Il gestore del canale di segnalazione interna comunica l'identità del segnalante solo nei casi espressamente previsti dalla legge • E' possibile effettuare segnalazioni in forma anonima • Gli sviluppatori della piattaforma non hanno alcuna forma di accesso ai dati, che risultano conservati in modalità crittografata • Il sistema mette a disposizione del segnalante appositi codici di accesso alla propria segnalazione • In caso di condivisione della piattaforma (legalmente consentita per i comuni diversi dai capoluoghi di provincia) si procede con accordo di contitolarità
Sicurezza della piattaforma	La piattaforma è dotata dei seguenti requisiti di sicurezza e conformità Certificazioni di Servizio - ISO/IEC 27001 - ISO/IEC 27017 - ISO/IEC 27018 - CSA STAR Self-Assessment - CAIQ Standard utilizzati nell'applicativo: - Metodologia di programmazione sicura su riferimento OWASP - Linguaggi utilizzati: Python / Javascript - Accessibilita conforma standard WAI-ARIA - Crittografia dei dati basasta su protocolli standard: AES/PGP/Curve25519/XSalsa20/Poly1305 - Crittografia delle connessioni HTTPS basata su TLSV1.2 e TLSV1.3 - Utilizzo del protocollo Tor per l'implementazione del piu avanzato livello di anonimato tecnologico al passo con lo stato dell'arte di settore.
Valutazione finale sul rischio residuo	**In riferimento all'analisi dei rischi ed alle misure di sicurezza adottate il rischio residuo legato al trattamento risulta: ACCETTABILE**

Nell'adozione delle suddette misure si è tenuto in debita considerazione il contenuto dell' Art.13 del Decreto Whistleblowing "Trattamento dei dati personali" prescrive che:

1. Ogni trattamento dei dati personali, compresa la comunicazione tra le autorità competenti, previsto dal presente decreto, deve essere effettuato a norma del regolamento (UE) 2016/679, del decreto legislativo 30 giugno 2003, n. 196 e del decreto legislativo 18 maggio 2018, n. 51. La comunicazione di dati personali da parte delle istituzioni, degli organi o degli organismi dell'Unione europea è effettuata in conformità del regolamento (UE)2018/1725.

2. I dati personali che manifestamente non sono utili al trattamento di una specifica segnalazione non sono raccolti o, se raccolti accidentalmente, sono cancellati immediatamente.

3. I diritti di cui agli articoli da 15 a 22 del regolamento (UE) 2016/679 possono essere esercitati nei limiti di quanto previsto dall'articolo 2 -undecies del decreto legislativo 30 giugno 2003, n. 196.

4. I trattamenti di dati personali relativi al ricevimento e alla gestione delle segnalazioni sono effettuati dai soggetti di cui all'articolo 4, in qualità di titolari del trattamento, nel rispetto dei princìpi di cui agli articoli 5 e 25 del regolamento (UE) 2016/679 o agli articoli 3 e 16 del decreto legislativo n. 51 del 2018, fornendo idonee informazioni alle persone segnalanti e alle persone coinvolte ai sensi degli articoli 13 e 14 del medesimo regolamento (UE) 2016/679 o dell'articolo 11 del citato decreto legislativo n. 51 del 2018, nonché adottando misure appropriate a tutela dei diritti e delle libertà degli interessati.

5. I soggetti del settore pubblico e i soggetti del settore privato che condividono risorse per il ricevimento e la gestione delle segnalazioni, ai sensi dell'articolo 4, comma 4, determinano in modo trasparente, mediante un accordo interno, le rispettive responsabilità in merito all'osservanza degli obblighi in materia di protezione dei dati personali, ai sensi dell'articolo 26 del regolamento (UE) 2016/679 o dell'articolo 23 del decreto legislativo n. 51 del 2018.

6. 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 d'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.

11) Consultazione delle parti

Nello sviluppo del Regolamento di gestione delle segnalazioni il Titolare ha consultato i seguenti soggetti:

◎ Gestore del canale di segnalazione
◎ Collaboratore interno
◎ Organismo di vigilanza / altro organo di controllo

12) Esito della valutazione di impatto

La seguente tabella riassume le conclusioni della valutazione di impatto condotta, definendo la conformità normativa (o la necessità di consultazione preliminare dell'Autorità Garante) del trattamento in oggetto.

OBIETTIVO DI ANALISI	RISULTATO	NOTE
Il trattamento è basato su di un corretto principio di liceità?	◉ Sì ◎ No ◎ N/A	GDPR, Art.6 (c)
La finalità è determinata, esplicita e legittima?	◉ Sì ◎ No ◎ N/A	Adempimenti di legge
I dati trattati sono adeguati, pertinenti e limitati?	◉ Sì ◎ No ◎ N/A	
I dati sono conservati per tempi coerenti con la finalità della raccolta?	◉ Sì ◎ No ◎ N/A	
I soggetti esterni coinvolti nel trattamento prestano adeguate garanzie?	◉ Sì ◎ No ◎ N/A	
I trasferimenti all'estero avvengono conformità al Capo V del GDPR?	◎ Sì ◎ No ◉ N/A	
Sono fornite adeguate informazioni agli interessati?	◉ Sì ◎ No ◎ N/A	
Gli interessati possono esercitare i diritti di cui agli art.15-21 del GDPR?	◎ Sì ◉ No ◎ N/A	Diritto limitato da Decreto
I rischi per i diritti e le libertà fondamentali degli interessati sono adeguatamente analizzati?	◉ Sì ◎ No ◎ N/A	
Le misure di sicurezza poste a tutela dei dati sono in grado di limitare i rischi ad un livello residuo accettabile?	◉ Sì ◎ No ◎ N/A	
Sono state consultate le parti coinvolte nel processo di trattamento?	◉ Sì ◎ No ◎ N/A	
Le parti coinvolte nel processo di trattamento concordano con le valutazioni di impatto?	◉ Sì ◎ No ◎ N/A	

CONCLUSIONE DELLA VALUTAZIONE DI IMPATTO

◉ **Il trattamento in oggetto può iniziare/proseguire**

(il livello di rischio è correttamente attenuato da adeguate misure di sicurezza, che garantiscano un livello di rischio residuo accettabile)

La presente valutazione di impatto sarà oggetto di opportuna revisione qualora intercorressero significativi cambiamenti nei profili oggetto di analisi.