COMUNE DI CORATO

DELIBERAZIONE DELLA GIUNTA COMUNALE N° 8 del 12/01/2024

OGGETTO: APPROVAZIONE VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA – DATA PROTECTION IMPACT ASSESSMENT) AI SENSI DEL REGOLAMENTO UE N. 679/2016 - PROCESSO DI GESTIONE DEL WHISTLEBLOWING.

L'anno 2024 il giorno 12 del mese di Gennaio alle ore 13:27, nella sede del Comune si è riunita la Giunta Comunale. Alla seduta risultano presenti:

N°	Nome	Qualifica	Presente	Assente
1	DE BENEDITTIS CORRADO NICOLA	Sindaco	SI	
2	MARCONE BENIAMINO	Assessore	SI	
3	ADDARIO FELICE	Assessore	SI	
4	ADDARIO LUISA	Assessore		SI
5	BUCCI CONCETTA	Assessore	SI	
6	SCISCIOLI GENNARO	Assessore	SI	
7	SINISI VINCENZO	Assessore	SI	
8	VARESANO ANTONELLA	Assessore	SI	

PRESENTI: 7 ASSENTI: 1

Il Sindaco Corrado Nicola De Benedittis, constatato il numero legale degli intervenuti e la regolarità della seduta dichiara aperta la seduta e invita la Giunta Comunale a trattare l'argomento in oggetto sulla cui proposta sono stati acquisiti i prescritti pareri ai sensi del TUEL.

Partecipa alla seduta il Segretario Generale Dott.ssa Marianna Aloisio.

LA GIUNTA COMUNALE

PREMESSO che:

1. con il decreto legislativo n. 24 del 10 marzo 2023 (in GURI 15/3/2023 n. 63), efficace dal 15 luglio, viene data attuazione alla direttiva UE 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione o delle normative nazionali;
2. l'art. 2 del d.lgs. n. 24/2023 definisce, in modo compiuto, quali siano le violazioni, oggetto di segnalazione, rilevanti ai fini dell'applicazione delle tutele;
3. l'art. 4, comma 1, del d.lgs. 24/2023 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, ai sensi del presente articolo, 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. I modelli di organizzazione e di gestione, di cui all'articolo 6, comma 1, lettera a), del decreto legislativo n. 231 del 2001, prevedono i canali di segnalazione interna di cui al presente decreto";
4. l'art. 4, comma 2, del d.lgs. 24/2023 stabilisce che "2. La gestione del canale di segnalazione è affidata a una persona o a un ufficio interno autonomo dedicato e con personale specificamente formato per la gestione del canale di segnalazione, ovvero è affidata a un soggetto esterno, anch'esso autonomo e con personale specificamente formato";

CONSIDERATO che ai sensi dell'art 4 comma 5 del D.lgs. 24/2023 "soggetti del settore pubblico cui sia fatto obbligo di prevedere la figura del responsabile della prevenzione della corruzione e della trasparenza, di cui all'articolo 1, comma 7, della legge 6 novembre 2012, n. 190, affidano a quest'ultimo, anche nelle ipotesi di condivisione di cui al comma 4, la gestione del canale di segnalazione interna";

PRESO ATTO che il Comune di Corato, ai fini di tutelare la riservatezza delle persone che segnalano violazioni ai sensi dell'art. 2 del d.lgs. 24/2023, si è dotato di una piattaforma che si avvale di idonei strumenti di crittografia;

VISTA la Piattaforma applicativa di Whistleblowing Solutions Impresa Sociale S.r.l. con sede in Viale Abruzzi 13/A, 20131, Milano, C.F. e P.IVA 09495830961, conforme in modo nativo alla normativa vigente, in particolare alle Linee guida in materia di Whistleblowing (L. 179/17) ed ai modelli organizzativi (D.Lgs. 231/01) Privacy – GDPR 2016/679;

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:
1. della portata della condivisione e della raccolta di dati personali significativi;
2.della tecnologia attuale che 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;
3. della tecnologia che ha trasformato l'economia e le relazioni sociali e che 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;

RICORDATO che:
1. tale evoluzione ha indotto l'Unione Europea ad adottare il Regolamento (UE) 2016/679, 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"), entrato in vigore ufficialmente in data 24 maggio 2016, e diventato definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;
2.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;

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:
1. una "determinazione" preliminare 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;
PRECISATO che la DPIA (Data Protection Impact Assessment) è una procedura prevista dall'art. 35 del Regolamento UE 206/679 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;

RILEVATO che:
1.la DPIA deve essere condotta prima di procedere al trattamento e che deve comunque essere previsto un suo riesame periodico;
2.è previsto l'obbligo in capo ai titolari di consultare l'Autorità di controllo nel caso in cui 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;
3.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, fermo 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 n. 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;

RICORDATO che:
- Questo ente, in ottemperanza alla Legge 179/2017 sul Whistleblowing, si è dotato di una piattaforma applicativa che consente di gestire il processo di segnalazione di illeciti rispettando le disposizioni dell'Autorità Nazionale per l'Anticorruzione e che è quindi necessario formulare una Valutazione di Impatto per la nuova procedura;
- la piattaforma applicativa individuata è quella fornita da Whistleblowing Solutions Impresa Sociale S.r.l. con sede in Viale Abruzzi 13/A, 20131, Milano, C.F. e P.IVA 09495830961 che è stata nominata quale Responsabile del Trattamento dei dati;

VISTI:
1.la Legge 190/2012 "Disposizioni per la prevenzione e la repressione della corruzione e dell'illegalità nella pubblica amministrazione";
2.la Legge 179/2017 sul Whistleblowing, a tutela del dipendente pubblico e privato, che prevede che sia predisposto "almeno un canale alternativo di segnalazione idoneo a garantire, con modalità informatiche, la riservatezza dell'identità del segnalante";
3. il Regolamento ANAC del 01 luglio 2020 per la gestione delle segnalazioni e per l'esercizio del potere sanzionatorio in materia di tutela degli autori di segnalazioni di illeciti o irregolarità di cui siano venuti a conoscenza nell'ambito di un rapporto di lavoro di cui all'art. 54 bis Decreto legislativo
n. 165/2001;
4.il Piano Nazionale Anticorruzione PNA 2019 Delibera ANAC n. 1064 del 13 novembre 2019: il RPCT, oltre a ricevere e prendere in carico le segnalazioni, pone in essere gli atti necessari ad una prima attività di verifica e di analisi delle segnalazioni ricevute da ritenersi obbligatoria in base al comma
6 dell'art. 54-bis del D.Lgs. n. 165/2001;
5.la delibera ANAC n. 469/2021, che contiene le "Linee guida in materia di tutela degli autori di segnalazioni di reati o irregolarità di cui siano venuti a conoscenza in ragione di un rapporto di lavoro, ai sensi dell'art. 54-bis, del d.lgs. 165/2001 (c.d. whistleblowing)", con la chiara indicazione che le segnalazioni, al fine di tutelare il segnalante, debbano essere trattate con sistemi informatizzati e crittografici;
6. il decreto legislativo n. 24 del 10 marzo 2023 (in GURI 15/3/2023 n. 63), che dà attuazione alla direttiva UE 2019/1937 riguardante la protezione delle persone che segnalano violazioni del diritto dell'Unione o delle normative nazionali ed ha abrogato dal 15 luglio 2023 l'art. 54-bis del d.lgs. 165/2001, aggiunto dalla legge 190/2012 e riscritto dalla legge 179/2017;

DATO ATTO che il responsabile del procedimento è il Segretario comunale Dott.ssa Marianna Aloisio e che lo stesso, 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;

RITENUTO di approvare la valutazione di impatto sulla protezione dei dati (dpia – data protection impact assessment), in ottemperanza alle disposizioni normative in vigore;

ACQUISITO il parere favorevole in ordine alla regolarità tecnica, ai sensi dell'articolo 49, comma 1, del D.Lgs. 18.08.2000 n. 267;

VISTI:
- Il vigente Statuto comunale;
- il D.lgs. n. 267/2000 e ss.mm.ii.;
Con voti unanimi

DELIBERA

Le premesse formano parte integrante e sostanziale al presente atto

1. di approvare la Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, corredata del parere favorevole del DPO, allegati alla presente per formarne parte integrante e sostanziale, ma esclusa dalla pubblicazione in quanto contenenti informazioni relative alle misure di sicurezza che devono restare di esclusivo appannaggio del titolare del trattamento, nonché dati tutelati da segreto aziendale;
2. di disporre che al presente provvedimento venga assicurata:
- la pubblicità legale con pubblicazione all'Albo Pretorio;
- 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 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;
4. di rendere, con separata e unanime votazione palese favorevole, il presente atto immediatamente esecutivo ai sensi dell'art. 134, 4° comma - T.U. 267/2000, al fine di provvedere tempestivamente alle attività conseguenti.

Il presente verbale viene letto, confermato e sottoscritto

Il Sindaco	Il Segretario Generale
Corrado Nicola De Benedittis	Dott.ssa Marianna Aloisio

(atto firmato digitalmente ai sensi del D.Lgs. n. 82/2005)