Comune di Alassio

Riviera dei Fiori

Verbale di deliberazione di Giunta Comunale

N° 181 di Registro Seduta del 13/07/2023

Oggetto: Approvazione versione n. 2 della valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016.

L'anno duemilaventitre, il giorno tredici del mese di Luglio alle ore 13:45, nella solita sala delle riunioni, previo esaurimento delle formalità prescritte dall'art. 50 del Testo Unico delle Leggi sull'Ordinamento degli Enti Locali, D.Lgs. 18 agosto 2000, n° 267, si è riunita la Giunta Comunale con l'intervento del Signori:

Nominativo	*Qualifica*	*Pres.*	*Ass.*
MELGRATI MARCO	***Sindaco***	***SI***	
GALTIERI ANGELO	***Assessore***	***SI***	
GIANNOTTA FRANCA	***Assessore***	***SI***	
INVERNIZZI ROCCO	***Assessore***	***SI***	
MORDENTE PATRIZIA	***Assessore***	***SI***	
ZAVARONI LORETTA	***Assessore***		***SI***

Partecipa alla seduta il Segretario Generale **Dott.ssa Roberta Ramoino.**

Assume la Presidenza **Melgrati Marco** in qualità di **Sindaco** che, riconosciuta la legalità dell'adunanza, dichiara aperta la seduta ed invita i presenti a deliberare in merito all'oggetto su indicato.

LA GIUNTA COMUNALE

Su proposta e relazione del Sindaco, quale rappresentante legale dell'Ente, supportato dall'Assessore all'Informatica, Dott. Rocco Invernizzi;

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 (di seguito solo "GDPR"), nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

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 206/679 (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 nel caso in cui le misure tecniche e organizzative da loro stessi individuate per mitigare l´impatto del trattamento, non siano sufficienti - ovvero, 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:

- 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 numeri 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 WP 248, 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;

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:
- 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;

DATO ATTO che il responsabile del procedimento, è il Segretario generale 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;

DATO ATTO che:

- il procedimento di adozione e approvazione della Valutazione d'impatto sulla protezione dei dati (DPIA) e il presente provvedimento, sono riconducibili al processo "gestione banche dati", mappato dal PTPCT;
- i controlli interni sono effettuati secondo il Regolamento per la disciplina dei controlli interni approvato con deliberazione n. 3/2013;
- il Piano Triennale di Prevenzione della corruzione, integrato con il piano per la trasparenza, viene annualmente approvato e rendicontato; non sono stati sollevati rilievi sulla sua applicazione;

VISTI:

- 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 interno dell'Ente;
- Circolari e direttive del RPC;

RICHIAMATO il Testo Unico delle Leggi sull'ordinamento degli EE. LL., approvato con D.Lgs. 18/08/2000, n° 267;

ACCERTATA la regolarità tecnica ai sensi dell'art. 49 del D.Lgs. 267/2000;

A voti unanimi favorevoli legalmente espressi,

DELIBERA

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

1. DI APPROVARE la versione n. 2 della Valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016, conservata agli atti di questo Ente.

2. DI DISPORRE che al presente provvedimento venga assicurata la pubblicità legale con pubblicazione all'Albo Pretorio, nonché 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.

5. DI DARE COMUNICAZIONE della presente deliberazione ai Capi Gruppo Consiliari ai sensi dell'Articolo 125 del Decreto Legislativo 18 agosto 2000, n. 267.

Successivamente, su proposta del Sindaco,

LA GIUNTA COMUNALE

ATTESA l'urgenza;

VISTO l'art. 134, comma 4, del Testo Unico delle Leggi sull'ordinamento degli EE. LL., approvato con D.Lgs. 18/08/2000 n° 267;

A voti unanimi favorevoli legalmente espressi,

DELIBERA

Di dichiarare il presente provvedimento immediatamente eseguibile.

Letto, approvato e sottoscritto:

IL SINDACO	IL SEGRETARIO GENERALE
Melgrati Marco	Dott.ssa Roberta Ramoino

Contrassegno Elettronico

TIPO QR Code

IMPRONTA (SHA-256): 0119e2f00d10edb3fb142713788749fa8dd0db3c63fad5531bf4eabccf3dcc0e

Firme digitali presenti nel documento originale

Roberta Ramoino
MARCO MELGRATI

Dati contenuti all'interno del Contrassegno Elettronico

Delibera di Giunta N.181/2023
Data: 13/07/2023
Oggetto: Approvazione versione n. 2 della valutazione d’impatto sulla protezione dei dati (DPIA) ai sensi del Regolamento (UE) n.679/2016.

Ai sensi degli articoli 23-bis e 23-ter del d.lgs.vo n. 82/2005 e s.m.i., si attesta che il presente documento, estratto in automatico dal sistema gestione documentale del COMUNE DI ALASSIO, è conforme al documento elettronico originale, predisposto e conservato in conformità alle regole tecniche di cui all'articolo 71.

ica del Contrassegno Elettronico

URL: http://www.timbro-digitale.it/GetDocument/GDOCController?qrc=88b19058e9ffb91c_p7m&auth=1

ID: 88b19058e9ffb91c