



COMUNE DI INDUNO OLONA
Provincia di Varese

VERBALE DI DELIBERAZIONE DELLA GIUNTA COMUNALE

Deliberazione n. 98 del 19/10/2026

OGGETTO: APPROVAZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA), REDATTA AI SENSI DELL' ART. 35 DEL REGOLAMENTO UE 2016/679 (GDPR)

L'anno **duemilaventisei** addì **diciannove** del mese di **ottobre** alle ore **16:00** nella sala giunta comunale, previa l'osservanza di tutte le formalità prescritte dalla vigente normativa, si sono riuniti i componenti di questa Giunta Comunale nelle persone dei Signori:

CASTELLI GIORGIO	SINDACO	Presente
BRENNA ANDREA	VICE SINDACO	Presente
MEZZALIRA MARCO	ASSESSORE	Presente
BORTOLI AURORA	ASSESSORE	Presente
GANDOLLA RAIMONDO	ASSESSORE	Assente
GORONE CHIARA	ASSESSORE	Presente

Presenti n. 5

Assenti n. 1

Partecipa con le funzioni di legge, il Segretario Generale dott.ssa Margherita Taldone.

Presiede la seduta, nella sua qualità di SINDACO, l'Ing. Giorgio Castelli che dichiara valida la seduta per la trattazione dell'oggetto sopra indicato.

OGGETTO: APPROVAZIONE DELLA VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA), REDATTA AI SENSI DELL'ART. 35 DEL REGOLAMENTO UE 2016/679 (GDPR)

LA GIUNTA COMUNALE

RILEVATO che la protezione delle persone fisiche, anche con riguardo al trattamento dei dati di carattere personale, è un diritto soggettivo 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;

RICORDATO, quindi, che le persone fisiche devono avere il controllo costante dei dati personali che li riguardano, tenuto conto della rapidità dell'evoluzione tecnologica comporta nuove sfide per la protezione dei dati personali, tenuto conto che:

- 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;
- la tecnologia ha trasformato l'economia e le relazioni sociali facilitando ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, pertanto, è necessario garantire 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, che ha abrogato la direttiva 95/46/CE;

RICORDATO 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, conforme allo sviluppo tecnologico e digitale sempre più impattante;

VISTO il D.Lgs. 196/2003, Codice in materia di protezione dei dati personali, 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 D.P.I.A. (*Data Protection Impact Assessment*) è una procedura prevista dall'art. 35 del Regolamento UE 2016/679 (GDPR) del 27.04.2016 nel caso dei sistemi di videosorveglianza come quello di cui dispone il Comune di Induno Olona che mira a rispondere adeguatamente alle suddette esigenze, valutando 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 del trattamento, 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 del trattamento, 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;
- trattamenti su larga scala di dati aventi carattere estremamente personale, come i 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;
- 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 (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;
- 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;

DATO ATTO che:

- il responsabile del procedimento relativo è il responsabile del Settore Vigilanza e Controllo - comandante della P.L. 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;
- in merito alla D.P.I.A. allegata alla presente deliberazione, è stato acquisito il parere favorevole del DPO (Data Protection Officer) in data 21.09.2026, con num. di protocollo generale 12719;

VISTI:

- la Legge n. 241/1990;
- il D.Lgs. n. 196/2003;
- il D.Lgs. n. 33/2013;
- il Regolamento (UE) n. 679/2016;
- le Linee-guida sui responsabili della protezione dei dati (RPD) – WP243, adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;

- le Linee-guida sul diritto alla “portabilità dei dati” - WP242, adottate dal Gruppo di lavoro Art. 29 il 13 dicembre 2016;
- le 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;
- le 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;
- le Linee guida elaborate dal Gruppo Art. 29 in materia di processi decisionali adottate dal Gruppo di lavoro Art. 29 il 6 febbraio 2018;
- le 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;
- lo Statuto Comunale;
- il Regolamento comunale sulla disciplina dei sistemi di videosorveglianza comunale, approvato con delibera del Consiglio Comunale n. 8 del 23.02.2026 ;

RICHIAMATO l'art. 48 (competenze delle giunte) del Testo Unico EE. LL., D.Lgs. 18/08/2000, n. 267;

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

A voti unanimi favorevoli legalmente espressi,

DELIBERA

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

1. Di approvare l'allegata Valutazione d'impatto sulla protezione dei dati (DPIA), redatta 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 pubblicazione sul sito web istituzionale, secondo criteri di facile accessibilità, completezza e semplicità di consultazione nella sezione “Amministrazione trasparente”.
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 dare mandato al Responsabile del Settore Vigilanza e Controllo di procedere alla adozione di tutti gli atti necessari e conseguenti al presente atto;

Di dichiarare, con unanime, favorevole, successiva e separata votazione palesamente espressa, la presente deliberazione immediatamente eseguibile ai sensi dell'art. 134, 4° comma del D.Lgs. 18/08/2000, n. 267.



COMUNE DI INDUNO OLONA
Provincia di Varese

Letto, approvato e sottoscritto digitalmente ai sensi dell'art. 21 D.L.gs n 82/2005 e s.m.i.

Verbale n. **41** del **19.10.2026**

IL SINDACO
Ing. Giorgio Castelli

IL SEGRETARIO GENERALE
Dott.ssa Margherita Taldone