Comune di Nichelino

Città Metropolitana di Torino

VALUTAZIONE DI IMPATTO

sulla protezione dei dati trattati nella gestione

del sistema di videosorveglianza

Articolo 35 del Regolamento generale per la protezione dei dati

(RGPD - REGOLAMENTO - UE - 2016/679)

Il documento è stato redatto, in collaborazione con il RPD, in data 6 Dicembre 2023.

Approvato con Deliberazione della Giunta n. 147 del 12.12.2023

Responsabile della Protezione dei Dati (RPD-DPO)

Gruppo Gaspari – Servizio privacy

Siamo contattabili

Via e-mail: privacy@gaspari.it

Via PEC: privacy@pec.egaspari.net

Via Posta ordinaria: Grafiche E.Gaspari Srl, Via M. Minghetti - 18, 40057, Cadriano di Granarolo Emilia (Bologna)

Via telefono: 051-763201

1.1. Premesse normative

Regolamento generale per la protezione dei dati (RGPD - REGOLAMENTO - UE - 2016/679)

Articolo 35 Valutazione d'impatto sulla protezione dei dati

1. 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 può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi***.

2. Il titolare del trattamento, allorquando svolge una valutazione d'impatto sulla protezione dei dati, si consulta con il responsabile della protezione dei dati, qualora ne sia designato uno.

3. La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti:

a) *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;*

b) *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;*

c) *la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.*

4. L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al Comitato di cui all'articolo 68 GDPR[1].

---

[1] *Il Garante della Privacy italiano ha emanato un "**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 - 11 ottobre 2018** - (Gazzetta Ufficiale Serie Generale n. 269 del 19 novembre 2018)" - In questo elenco sono previste le seguenti fattispecie:*

- *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*

5. L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.

6. Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.

7. La valutazione contiene 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.*

8. Nel valutare l'impatto del trattamento effettuato dai relativi titolari o responsabili è tenuto in debito conto il rispetto da parte di questi ultimi dei codici di condotta approvati di cui all'articolo 40, in particolare ai fini di una valutazione d'impatto sulla protezione dei dati.

Sostanzialmente, le norme predette, stabiliscono 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 Titolare, coadiuvato dal Responsabile della protezione dei dati, se designato, è obbligato a svolgere

---

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 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.*

una valutazione di impatto prima di dare inizio al trattamento (DPIA – Data protection impact assessment o anche PIA–Privacy Impact Assessment).

Nel quadro normative di riferimento, la DPIA costituisce uno degli elementi di maggiore rilevanza, perchè esprime chiaramente la responsabilizzazione (accountability) del Titolare nei confronti del trattamento da lui effettuato.

Il titolare infatti è tenuto, non soltanto, a garantire il rispetto delle disposizioni previste dal GDPR, ma anche a dimostrare adeguatamente in che modo garantisce la sua osservanza.

Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video Versione 2.0 - Adottate il 29 gennaio 2020

10 VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

136. Ai sensi dell'articolo 35, paragrafo 1, del RGPD, i titolari del trattamento sono tenuti a condurre valutazioni d'impatto sulla protezione dei dati quando una determinata tipologia di trattamenti può presentare un rischio elevato per i diritti e le libertà delle persone fisiche. L'articolo 35, paragrafo 3, lettera c), del RGPD stabilisce che i titolari del trattamento sono tenuti a effettuare valutazioni d'impatto sulla protezione dei dati se il trattamento consiste nella sorveglianza sistematica di una zona accessibile al pubblico su larga scala. Inoltre, ai sensi dell'articolo 35, paragrafo 3, lettera b), del RGPD, è necessaria una valutazione d'impatto sulla protezione dei dati anche quando il titolare intende trattare categorie particolari di dati su larga scala.

137. Le linee guida in materia di valutazione d'impatto sulla protezione dei dati (27) forniscono ulteriori indicazioni ed esempi più dettagliati relativi alla videosorveglianza (ad esempio, per quanto riguarda «l'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade»).

L'articolo 35, paragrafo 4, del RGPD prevede che ogni autorità di controllo pubblichi un elenco delle tipologie di trattamento soggette obbligatoriamente a valutazione d'impatto sulla protezione dei dati nel rispettivo Stato membro. Di norma, questi elenchi sono reperibili sui siti web delle autorità. Date le finalità tipiche della videosorveglianza (protezione delle persone e dei beni, individuazione, prevenzione e controllo di reati, raccolta di elementi di prova e identificazione biometrica di soggetti sospetti), è ragionevole supporre che molti casi di videosorveglianza richiederanno una valutazione d'impatto sulla protezione dei dati. I titolari del trattamento dovrebbero quindi consultare attentamente questi documenti al fine di determinare se tale valutazione sia necessaria e, in tal caso, al fine di effettuarla. L'esito della valutazione d'impatto sulla protezione dei dati dovrebbe determinare la scelta del titolare del trattamento sulle misure di protezione dei dati implementate.

138. È inoltre importante ricordare che, ove i risultati della valutazione d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato nonostante le misure di sicurezza pianificate dal titolare, occorrerà consultare l'autorità di controllo competente prima di procedere al trattamento. Le disposizioni in materia di consultazioni preventive sono contenute nell'articolo 36 del RGPD.

1.2. Panoramica del sistema di videosorveglianza

Il trattamento preso in considerazione è relativo al trattamento dei dati raccolti dall'impianto di videosorveglianza del Comune di Nichelino (TO).

In particolare ai fini della:

- tutela della sicurezza urbana nei luoghi pubblici o aperti al pubblico;
- tutela della sicurezza stradale, per monitorare la circolazione lungo le strade del territorio comunale e fornire ausilio in materia di polizia amministrativa in generale;
- tutela del patrimonio comunale, per presidiare gli accessi agli edifici comunali, dall'interno o dall'esterno e le aree adiacenti o pertinenti ad uffici od immobili comunali;
- tutela ambientale del territorio ed in particolare scoraggiare e prevenire il fenomeno dell'abbandono di rifiuti, quando non risulta possibile, o si riveli inefficace, il ricorso a strumenti e sistemi di controllo alternativi.

In via incidentale:

- all'esigenza, per finalità di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali a norma del D.Lgs. n. 51/2018.

Ha disposto, nel rispetto della vigente normativa in materia e delle prescrizioni fornite dal Garante per la protezione dei dati personali, l'attivazione di un impianto di videosorveglianza urbana mediante l'installazione di telecamere debitamente segnalate. Le apparecchiature sono indirizzate verso aree pubbliche o soggette a servitù di pubblico passaggio nonché su beni di proprietà comunale, individuati in ragione delle esigenze di sicurezza urbana, tutela del patrimonio comunale, tutela della sicurezza stradale e del controllo ambientale e sono collocate nelle seguenti località.

LOCALIZZAZIONE Videocamere

CAM 1. Comitato San Quirico – Via Bengasi n.20, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 2. Comitato Sangone- Crocera – via Roma n.16, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 3. Comitato Oltrestazione – Via Gozzano n. 29, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 4. Comitato Boschetto – Piazza Pertini, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 5. Comitato Castello – Via Turati n.4, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 6. Comitato Kennedy – P.zza Madre Teresa di Calcutta, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 7. Teatro Superga – Via Superga n.44, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM. 8 Asilo Nido comunale – Via Cacciatori n.21/2, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 9. Giardino pubblico – Via Milano per finalità di tutela della sicurezza urbana;
CAM 10. Giardino pubblico – Via Juvarra ang. Via Giordano, per finalità di tutela della sicurezza urbana;
CAM 11. Giardino pubblico – Viale Kennedy ingresso Parrocchia San Vincenzo de Paoli, per finalità di tutela della sicurezza urbana;
CAM 12. Giardino pubblico – Via Galimberti, per finalità di tutela della sicurezza urbana;
CAM 13. Parco Miraflores – Via Pracavallo n. 62, per finalità di tutela della sicurezza urbana;
CAM 14. Cimitero comunale, ingressi e parcheggio Via Pateri, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 15. Biblioteca comunale, via Turati, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 16. Farmacia comunale – P.zza Aldo Moro, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 17. Informagiovani – Via Galimberti (Centro Grosa), per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 18. Anagrafe – Piazza Camandona, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 19. Palazzo del Municipio – Piazza Di Vittorio n.1, per finalità di tutela della sicurezza urbana e tutela del patrimonio;
CAM 20. Comando Polizia Municipale – Via Giusti n.2, per finalità di tutela della sicurezza urbana e tutela del patrimonio;

CAM 21. Impianto T-red, controllo violazioni passaggio con semaforo rosso, Via Torino ang. Via Martiri della Libertà, in entrambe le direzioni di marcia, tutela della sicurezza stradale;
CAM 22. Impianto T-red, controllo violazioni passaggio con semaforo rosso, Via Torino ang. Via Giusti, in entrambe le direzioni di marcia, tutela della sicurezza stradale;
CAM 23. Impianto T-red, controllo violazioni passaggio con semaforo rosso, Via Torino ang. Via Verdi, in entrambe le direzioni di marcia, tutela della sicurezza stradale;
CAM 24. Impianto T-red, controllo violazioni passaggio con semaforo rosso, Via Torino ang. Via Brescia, in entrambe le direzioni di marcia, tutela della sicurezza stradale;
CAM 25. Piazza Carlo Alberto dalla Chiesa, per finalità di tutela della sicurezza urbana;
CAM 26. Via Torino angolo Via Scarrone, per finalità di tutela della sicurezza urbana e stradale;
CAM 27. Via Torino angolo Via Vernea, per finalità di tutela della sicurezza urbana e stradale;
CAM 28. Largo delle Alpi angolo Via XXV Aprile, per finalità di tutela della sicurezza urbana e stradale;
CAM 29. Largo delle Alpi angolo Via Debouchè, per finalità di tutela della sicurezza urbana e stradale;
CAM 30. Largo delle Alpi angolo Via dei Cacciatori, per finalità di tutela della sicurezza urbana e stradale;
CAM 31. Ponte Sangone – Via Polveriera, per finalità di tutela della sicurezza urbana e stradale;
CAM 32. Ponte Sangone – Via Torino, per finalità di tutela della sicurezza urbana e stradale;

Accanto a tali impianti di videosorveglianza Il Comune di Nichelino, al fine di contrastare, scoraggiare e prevenire l'increscioso abbandono e smaltimento illecito dei rifiuti sul territorio, nonostante i numerosi controlli ambientali effettuati dalla Polizia Municipale, si avvale di un sistema di videosorveglianza realizzato mediante l'utilizzazione di fototrappole collocate, per un determinato tempo, in prossimità dei siti maggiormente a rischio (lungo le strade, e nelle loro pertinenze nonché nelle aree verdi).
Le fototrappole sono progettate per l'uso all'aperto e si innescano a seguito di qualsiasi movimento di essere umani o animali monitorata da un sensore ad alta sensibilità di movimento a infrarossi passivo, per scattare foto e video.

LOCALIZZAZIONE Fototrappole

CAM 33. Via Parri n.3 per finalità di tutela della sicurezza urbana e ambientale;
CAM 34. Via Colombetto ang. Piazza Giusti, per finalità di tutela della sicurezza urbana e ambientale;
CAM 35. Via Bengasi n.3 per finalità di tutela della sicurezza urbana e ambientale;

Infine a partire da maggio 2023 sono stati installati sul territorio cittadino n.6 Velobox, posti a prevenzione dell'eccessiva velocità dei veicoli in circolazione e contenitori dell'apparecchiatura ENVES di rilevamento della velocità istantanea, posti lungo i tratti periferici d'accesso alla città. A seguito di una serie di atti vandalici a carico delle predette strutture sono state installate nelle località sotto indicate delle videocamere mobili progettate per l'uso all'aperto che s'innescano a seguito di qualsiasi movimento avviene in prossimità dei Velobox, attraverso un monitoraggio da parte di un sensore ad alta sensibilità di movimento a infrarossi passivo, per riprodurre foto e video.

LOCALIZZAZIONE Videocamere mobili

CAM 36. Viale Pateri n.82, per finalità di tutela della sicurezza urbana e stradale;
CAM 37. Via Nenni n.26, per finalità di tutela della sicurezza urbana e stradale;
CAM 38. Strada Buffa n.90, per finalità di tutela della sicurezza urbana e stradale;
CAM 39. Via XXV Aprile n.152, per finalità di tutela della sicurezza urbana e stradale;
CAM 40. Viale Matteotti n.29, per finalità di tutela della sicurezza urbana e stradale;
CAM 41. Via Torino n. 275, per finalità di tutela della sicurezza urbana e stradale.

La registrazione, il trattamento e la conservazione delle immagini è effettuata dal Corpo di Polizia Municipale del Comune di Nichelino (TO).

TITOLARE DEL TRATTAMENTO:

Comune di Nichelino (TO), Piazza Di Vittorio n° 1 10042, Nichelino (TO)
Telefono (39) 011 68191 PEC: protocollo@cert.comune.nichelino.to.it

RESPONSABILE DELLA PROTEZIONE DATI:

Grafiche & Gaspari Srl
Telefono 051.763201
MAIL: privacy@gaspari.it
PEC: privacy@pec.egaspari.net

1.3 Accountability

Per il sistema di videosorveglianza, sono state prese una serie di misure necessarie a garantire un adeguato trattamento dei dati alla disciplina del GDPR e la loro sicurezza:

- *Disposizione n. 5 del 3 febbraio 2023,* del Comandante del Corpo di Polizia Municipale che ha individuato la prassi da seguire per l'accesso alle immagini di videosorveglianza ed il personale del Corpo di P.M. e della società alla quale è affidata la gestione e la manutenzione dell'impianto di videosorveglianza.
- *Cartelli di avviso di area sottoposta a videosorveglianza*, in linea con EDPB - Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video - adottate il 29 gennaio 2020.
- *Registro delle attività di trattamento relative al sistema di videosorveglianza,* ex articolo 2-quaterdecies del D.Lgs. n.196/2003, adottato con Determinazione n. 166 del 3 febbraio 2023, dove sono annotate le fasi di trattamento della videosorveglianza urbana e la modulistica VGS 1 e VSG2 di accesso e scarico delle immagini.

1.4 Individuazione e gestione del rischio

Per valutare quali rischi corrono i dati personali dei cittadini che vengono trattati dal titolare e dal responsabile del trattamento, bisogna individuare una serie di elementi che il Garante della Privacy italiano ha messo a fuoco in alcune diapositive pubblicate sul suo sito e che riproduciamo in parte qui di seguito

[https://www.garanteprivacy.it/documents/10160/0/Individuazione+e+gestione+del+rischio+-+Tutorial+-+slide.pdf/d2eb9375-c577-4ff3-b716-38cc703ec26f?version=1.0]:

Regolamento UE/2016/679

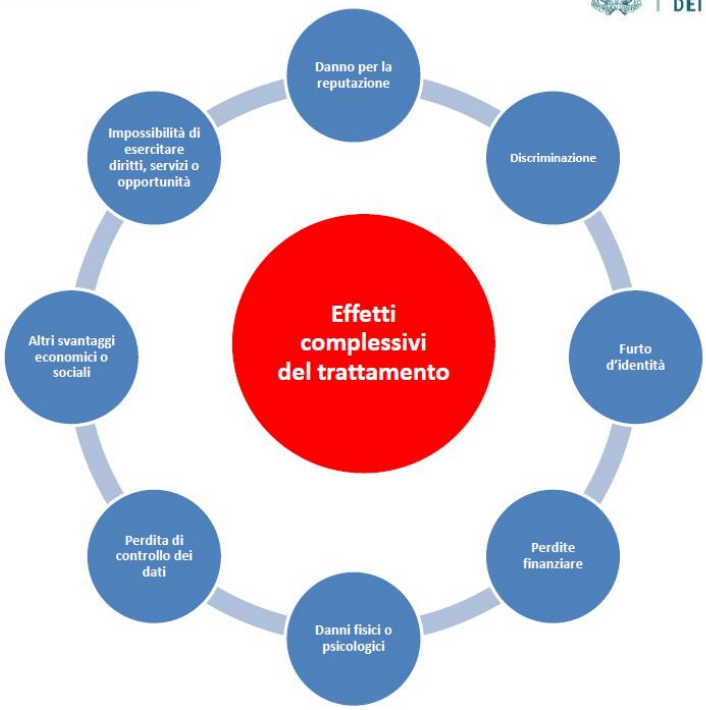
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

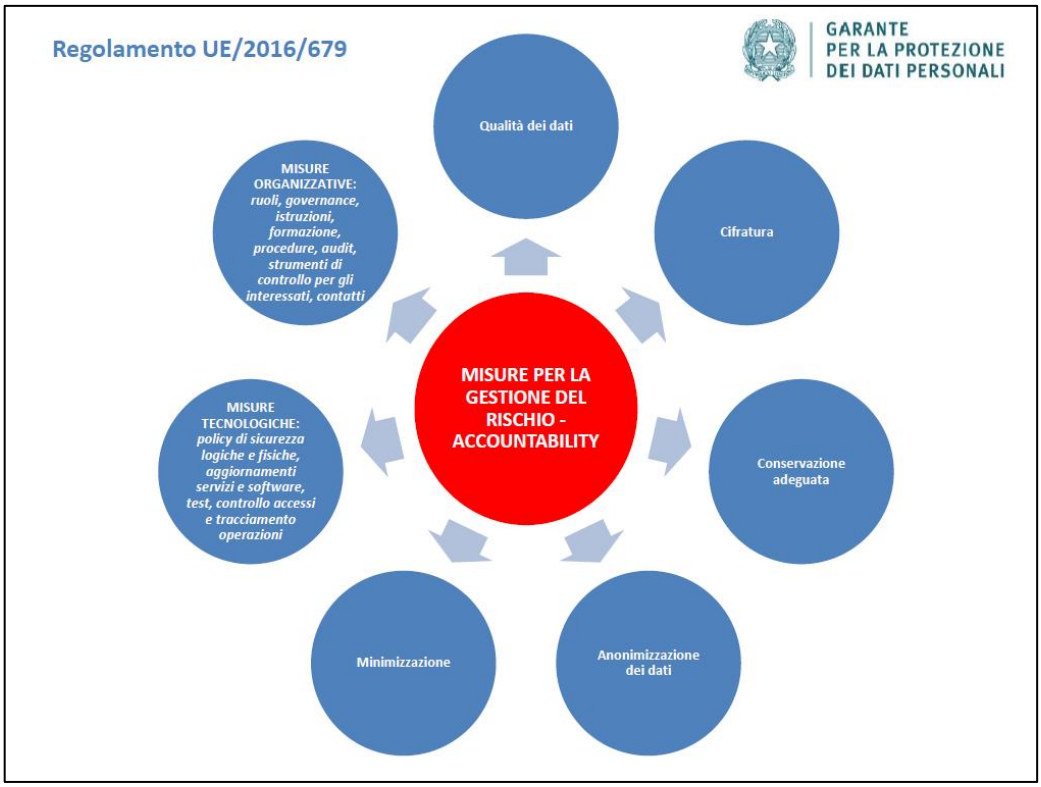
Aspetti riguardanti la sicurezza del trattamento

- **DISPONIBILITÀ**
  -distruzione
  -indisponibilità
  -perdita
- **INTEGRITÀ**
  -alterazione
- **RISERVATEZZA**
  -divulgazione
  -accesso

Regolamento UE/2016/679

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI





1.5 Modalità di valutazione di impatto per un comune

Tra le premesse normative e metodologiche che impongono l'adozione della DPIA abbiamo:

1. *Quando un trattamento di dati è massivo, come quello effettuato da un comune, sembrerebbe obbligatorio fare la PIA*
2. *Quando però un trattamento di dati è previsto e disciplinato da norme imperative o è effettuato nell'ambito di un pubblico interesse, come tutti i trattamenti di dati del comune, sembrerebbe escluso che debba essere sottoposto a PIA*
3. *I prodotti informatici in commercio e il software open source del Garante non sono predisposti per i comuni, ma per le piccole e medie imprese;*
4. *Sembra opportuno in questa prima fase di applicazione del RGPD, effettuare comunque una PIA anche se non obbligati*

Alla luce di tutto ciò, Il Comune di Nichelino relativamente al trattamento dei dati derivanti dall'impianto di videosorveglianza ha predisposto la presente DPIA, utilizzando il software open source "PIA" messo a disposizione dal CNIL (Autorità garante francese per la protezione dei dati personali), progetto a cui ha aderito successivamente l'Autorità garante italiana, inteso quale valido supporto ed indirizzo operativo, reperibile al link:

https://www.garanteprivacy.it/regolamentoue/DPIA#STRUMENTI

NB: I punteggi di ogni sezione sono parametrati su un valore minimo di 0 e un valore massimo di 30.

2. Risultati della rilevazione per la valutazione di impatto

Art. 35 del Regolamento generale per la protezione dei dati

(RGPD - REGOLAMENTO - UE - 2016/679)

Sezione 1: adempimenti di carattere generale

1. **Nomina del Responsabile della protezione dei dati?**

   Sì, con apposito atto

Punti 6 (*Sì= 6 – No = 0*)

2. **Comunicazione al Garante della Privacy della nomina del RPD?**

   Sì, in data 17/03/2021

Punti 6 (*Sì= 6 – No = 0*)

3. **Dati di contatto del RPD sono presenti sul sito istituzionale?**

   Sì, alla pagina https://comune.nichelino.to.it/privacy-policy/

Punti 6 (*Sì= 6 – No = 0*)

4. **I dati di contatto del RPD sono presenti sulle informative e sui cartelli informativi possi in prossimità delle telecamere adibite alla videosorveglianza?**

   Sì

Punti 6 (*Sì= 6 – No = 0*)

5. **Adottato un Registro dei trattamenti?**

   Si, consultabile all'indirizzo:
   https://comune.nichelino.to.it/wp-content/uploads/sites/56/2023/02/registro-trattamento-dati.pdf

Punti 6 (*Sì= 6 – No = 0*)

Tot. punti sez.1: 30

Sezione 2: - mappatura del rischio

6. Mappatura del Rischio relativo al trattamento dati sistema di videosorveglianza

COD.	Denominazione della banca dati personale	**Massimo30**

Il punteggio max di 30 si ottiene solo se il servizio è gestito direttamente dal comune, sommando questi elementi:

- *Max 10 se la banca dati è gestita in formato elettronico con apposito applicativo*
- *Max 10 se l'applicativo risponde a criteri di affidabilità*
- *Max 10 se gli operatori impiegati sono adeguatamente formati*

Banche dati personali dei servizi di vigilanza e controllo	
Videosorveglianza	
Criteri	Punteggio
Banca dati è gestita in formato elettronico con apposito applicativo	10
L'applicativo risponde a criteri di affidabilità	10
Gli operatori impiegati sono adeguatamente formati	10

Tot. punti sez. 2: 30

Sezione 3: misure di sicurezza fisiche

7. **Sono state adottate queste misure di sicurezza (archivi cartacei: registro degli eventi e degli accessi)?**

ID	Denominazione scheda registro	**1** punto per ogni misura
1.	Gli accessi nelle stanze in cui sono presenti archivi cartacei sono riservati	1
2.	L'accesso agli archivi cartacei è assicurato con una serratura	1
3.	Sono presenti antifurto	1
4.	Sono presenti sistemi antincendio, climatizzazione ambientale o deumidificazione	1
5.	E' stato redatto un registro d'archivio	1

8. **Sono state adottate queste misure di sicurezza (archivi informatici - HARDWARE)?**

ID	Denominazione scheda registro	**5** punti per ogni misura
1.	E' previsto un piano per il disaster recovery (AGID)	0
2.	E' stata fatta una virtualizzazione dei server	0
3.	E' prevista una rete cablata proprietaria (no WIFI)	5
4.	È presente un sistema di alimentazione elettrica ininterrotta (gruppo di continuità) per l'alimentazione dei server?	5
5.	I client sono PC o terminali riservati all'uso d'ufficio (no rimovibili)	5

Tot. punti sez. 3: 20

Sezione 4: misure di sicurezza logiche

9. Sono state adottate queste misure "logiche" di sicurezza per gli archivi informatici?

ID	Denominazione scheda registro	**Dare un punteggio da 0 a 3**
1.	È stato nominato un responsabile della transizione digitale (AGID)	3
2.	Il server è sotto protezione logica (password di accesso)	3
3.	Sono state assegnati ID – PW – e Credenziali differenziate e personali	3
4.	È presente un antivirus e/o firewall in grado di inibire la navigazione su siti e procedure pericolose	3
5.	È presente un sistema strutturato di copie di backup	1
6.	Il software in uso è licenziato e certificato	3
7.	Il software in uso è costantemente aggiornato	3
8.	Esiste una tracciatura dei log di accesso al server	3
9.	È stata fatta una virtualizzazione dei server	3
10.	È presente un sistema di crittografia dei dati	3

Tot. punti sez. 4: 28

Sezione 5: - gestione del dato e tutela dei diritti degli interessati

10. L'assetto attuale delle misure adottate permette?

ID	Denominazione scheda registro	**Dare un punteggio da 0 a 3****
1.	L'accesso ai propri dati da parte degli interessati, attraverso modalità di tutela dei dati nelle istanze di accesso generalizzato e documentale	3
2.	La minimizzazione dell'utilizzo dei dati e della loro richiesta	3
3.	Informazione adeguata tramite apposizione della cartellonistica in prossimità delle telecamere	3
4.	Evitare furti di identità	3
5.	La gestione tempestiva di un'eventuale data breach, qualora avvenga una violazione	3
6.	La predisposizione di misure analoghe alle proprie per i trattamenti eseguiti da terzi responsabili	3
7.	L'aver individuato anche implicitamente i compiti e le funzioni di ciascun addetto	3
8.	L'aver promosso iniziative di formazione e informazione per i cittadini	0
9.	L'aver promosso iniziative di formazione per i dipendenti	1
10.	L'aver adottato nel PTPCT idonee misure che bilancino trasparenza e riservatezza	3

** *Queste 10 misure sono degli obiettivi e, quasi sempre, richiedono un approccio graduale, pertanto il punteggio massimo è riconosciuto solo quando l'obiettivo è raggiunto al 100%; si dia un punteggio proporzionale minore, anche con l'uso dei decimali, per il raggiungimento parziale.*

Tot. punti sez. 5: 25

La rilevazione dei dati e l'assegnazione **provvisoria** dei punteggi è stata eseguita il 5 dicembre 2023 dal **Comandante della Polizia Municipale, dott*. Giustino Goduti*.**

L'apposito modello di rilevazione è stato trasmesso via mail, nella stessa data al RPD (Responsabile per la Protezione dei Dati): Gruppo Gaspari - servizio Privacy per l'inserimento nel gestionale, che ha assegnato i relativi punteggi **finali di seguito indicati.**

3. Risultati e prescrizioni della valutazione di impatto

3.1 Tabella riassuntiva (riportare i punteggi di ciascuna sezione):

Sez.	Denominazione della sezione	Punti
1	***adempimenti di carattere generale***	30
2	***mappatura del rischio***	30
3	***misure di sicurezza fisiche***	20
4	***misure di sicurezza logiche***	28
5	***gestione del dato e tutela dei diritti degli interessati***	25
Totale punteggio (somma da 1 a 5)		**133/150**

Misure da adottare	***Valutazione di impatto*** (*rappresentazione grafica*)				
Se il punteggio della sezione è in questo spazio la situazione è sicura, ma serve vigilare per mantenere i risultati raggiunti	**Da 25 a 30**				
Se il punteggio della sezione è in questo spazio la situazione è già accettabile, ma conviene agire su qualche misura, per consolidare	**Da 19 a 24**				
Se il punteggio della sezione è in questo spazio è utile agire su qualcuna delle misure	**Da 13 a 18**				
Se il punteggio della sezione è in questo spazio è necessario agire sulla maggior parte delle misure	**Da 7 a 12**				
Se il punteggio della sezione è in questo spazio è necessario agire su tutte le misure previste	**Da 0 a 6**				
Gradazione del rischio	Rischio massimo	Rischio elevato	Rischio medio	Rischio Limitato	Rischio Trascurabile

3.2 Prescrizioni del "validatore": il parere del DPO/RPD

Per il sistema di videosorveglianza, sono state prese tutte le misure necessarie a garantire un buon grado di sicurezza della banca dati: il personale designato al trattamento risulta formato, e sono state garantite misure adeguate d'informazione per i cittadini.

La sicurezza fisica, in relazione alla conservazione dei dati, può essere ulteriormente migliorata attuando una virtualizzazione del server adibito alla conservazione dei dati: tale misura rappresenta infatti un ulteriore elemento di contrasto alla prevenzione di eventuali "data breach". Una virtualizzazione dei server permetterebbe inoltre l'implementazione di un migliore sistema di ripristino dei dati in caso di danneggiamento o perdita, tramite un meccanismo di backup più sicuro.

Inoltre, al fine di migliorare la gestione del dato e tutela dei diritti degli interessati, anche alla luce della particolarità del trattamento oggetto della presente valutazione, si raccomanda la promozione di iniziative di informazione per i cittadini, aventi ad oggetto il tema dei diritti e dei doveri riguardanti il trattamento di dati personali.

Si ricorda infine la necessità di aggiornare frequentemente i software in uso per garantire uno standard di sicurezza elevato, e in generale un controllo costante dei sistemi di sicurezza adottati.