Comune di Oristano

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale aggiornata

2024

SOMMARIO

INTRODUZIONE

La presente DPIA - *Data Protection Impact Assessment*, valuta l'impatto che i trattamenti di dati personali effettuati dal Comune di Oristano hanno nei confronti dei diritti e libertà delle persone fisiche.

Il General Data Protection Regulation, Regolamento (UE) 2016/679 del 27 aprile 2016, prevede che il titolare del trattamento dei dati attui misure adeguate, analizzando e prevedendo misure di mitigazione dei rischi.

Il Garante per la Privacy, autorità di garanzia italiana, stabiliva con il provvedimento dell'8 aprile 2010, in materia di trattamento dei dati personali attraverso strumenti di videosorveglianza, di sottoporre a valutazione preventiva una serie di trattamenti di dati particolarmente invasivi eseguiti attraverso:
• sistemi di videosorveglianza dotati di software che analizzino dati biometrici e il riconoscimento delle persone;
• sistemi c.d. intelligenti in grado di rilevare automaticamente comportamenti o eventi anomali, segnalarli ed eventualmente registrarli;
• sistemi integrati di videosorveglianza;
• nei casi di trattamenti dove era necessario l'allungamento dei tempi di conservazione delle immagini oltre il termine massimo previsto.

Dopo l'entrata in vigore del Regolamento UE 2016/679, tutti i casi sopraelencati, (principio della *Accountability*) non hanno più necessità di una autorizzazione preventiva dell'autorità di garanzia, ma di una valutazione d'impatto effettuata dal titolare del trattamento, con il supporto del *Data Protection Officer* – DPO (art. 35 Regolamento UE 2016/679).

Per definire con maggior dettaglio e stabilire i trattamenti soggetti alla valutazione d'impatto sulla protezione dei dati sopradetti, il Garante per la Privacy ha emanato il provvedimento n. 467 del 10 ottobre 2018.

La valutazione di impatto del trattamento dei dati è un processo necessario ed utile per acquisire consapevolezza dei rischi connaturati al trattamento che si vuole porre in essere e per scegliere le misure tecniche e organizzative necessarie, da mettere in pratica, per ridurli.

Nella DPIA sono riportati quindi gli elementi fondamentali descrittivi del trattamento, il risultato della valutazione d'impatto derivante dall'analisi del rischio e le misure di mitigazione preventivamente valutate in merito all'esecuzione o meno del trattamento dati.

Tutti i risultati ottenuti nell'ambito della DPIA verranno dettagliati attraverso:
1. la descrizione del trattamento;
2. valutazione e analisi della necessità e proporzionalità del trattamento;
3. valutazione e gestione dei rischi derivanti dal trattamento;
4. acquisizione del parere del DPO *Data Protection Officer*.

La presente DPIA, sottoscritta dal Dirigente Comandante della Polizia Locale, approvata dalla Giunta Comunale, verrà successivamente sottoposta a parere del DPO Data Protection Officer del Comune di Oristano.

OBIETTIVO DEL DOCUMENTO

La DPIA ha come obiettivo quello di valutare l'impatto che hanno i trattamenti effettuati con i sistemi di videosorveglianza e tutti gli altri sotto descritti, connessi alle attività di Polizia Locale, posti in essere dal Comune di Oristano rispetto ai diritti e le libertà degli interessati.

Il presente documento quindi è stato svolto sia ai sensi dell'art. 35 del Regolamento (UE) 2016/679 e sia ai sensi dell'art. 23 del decreto legislativo 51/2018 per i trattamenti finalizzati alla prevenzione, indagine, accertamento, perseguimento di reati, esecuzione di sanzioni penali, prevenzione e salvaguardia della sicurezza pubblica, sia alla luce delle Linee guida WP29 del 4 ottobre 2017 "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" e sia delle Linee guida EDPB 3/2019 "sul trattamento dei dati personali attraverso dispositivi video".

Attraverso questa valutazione sono state analizzate e descritte le misure tecniche, organizzative e procedurali da adottare per un corretto trattamento dei dati. Sono descritti, inoltre, nella DPIA e nella Relazione Tecnica Operativa allegata alla presente, i livelli di rischi intrinseci ai trattamenti analizzati e le misure adottate per la mitigazione degli stessi.

A questo documento sono allegati tutti gli atti a comprova di quanto in esso è stato riportato ed è stato oggetto di valutazione.

DEFINIZIONI E ABBREVIAZIONI

- **Servizio:** utilizzo degli impianti di videosorveglianza e connessi all'esercizio delle attività di Polizia Locale, attivati nel territorio del Comune di Oristano

- **Titolare del trattamento:** in base all'art. 4 del GDPR è "*la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali*". Relativamente a questo documento il Titolare del trattamento è il Comune di Oristano;

- **Responsabile del trattamento:** Soggetto o Società di servizi nominata Responsabile del trattamento ai sensi dell'art. 28 del GDPR: "*1. Qualora un trattamento debba essere effettuato per conto del titolare del trattamento, quest'ultimo ricorre unicamente a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento e garantisca la tutela dei diritti dell'interessato. 2. Il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento. Nel caso di autorizzazione scritta generale, il responsabile del trattamento informa il titolare del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri responsabili del trattamento, dando così al titolare del trattamento l'opportunità di opporsi a tali modifiche. 3. I trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento. Il contratto o altro atto giuridico prevede, in particolare, che il responsabile del trattamento: a) tratti i dati personali soltanto su istruzione documentata del titolare del trattamento, anche in caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, salvo che lo richieda il diritto dell'Unione o nazionale cui è soggetto il responsabile del trattamento; in tal caso, il responsabile del trattamento informa il titolare del trattamento circa tale obbligo giuridico prima del trattamento, a meno che il diritto vieti tale informazione per rilevanti motivi di interesse pubblico; b) garantisca che le persone autorizzate al trattamento dei dati personali si siano impegnate alla riservatezza o abbiano un adeguato obbligo legale di riservatezza; c) adotti tutte le misure richieste ai sensi dell'articolo 32; d) rispetti le condizioni di cui ai paragrafi 2 e 4 per ricorrere a un altro responsabile del trattamento; e) tenendo conto della natura del trattamento, assista il titolare del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III; f) assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento; g) su scelta del titolare del trattamento, cancelli o gli restituisca tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancelli le copie esistenti, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati; e h) metta a disposizione del titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui al presente articolo e consenta e contribuisca alle attività di revisione, comprese le ispezioni, realizzati dal titolare del trattamento o da un altro soggetto da questi incaricato. Con riguardo alla lettera h) del*

primo comma, il responsabile del trattamento informa immediatamente il titolare del trattamento qualora, a suo parere, un'istruzione violi il presente regolamento o altre disposizioni, nazionali o dell'Unione, relative alla protezione dei dati. 4. Quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare del trattamento, su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del presente regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile. 5. L'adesione da parte del responsabile del trattamento a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare le garanzie sufficienti di cui ai paragrafi 1 e 4 del presente articolo. 6. Fatto salvo un contratto individuale tra il titolare del trattamento e il responsabile del trattamento, il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 del presente articolo può basarsi, in tutto o in parte, su clausole contrattuali tipo di cui ai paragrafi 7 e 8 del presente articolo, anche laddove siano parte di una certificazione concessa al titolare del trattamento o al responsabile del trattamento ai sensi degli articoli 42 e 43. 7. La Commissione può stabilire clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo e secondo la procedura d'esame di cui all'articolo 93, paragrafo 2. 8. Un'autorità di controllo può adottare clausole contrattuali tipo per le materie di cui ai paragrafi 3 e 4 del presente articolo in conformità del meccanismo di coerenza di cui all'articolo 63. 9. Il contratto o altro atto giuridico di cui ai paragrafi 3 e 4 è stipulato in forma scritta, anche in formato elettronico. 10. Fatti salvi gli articoli 82, 83 e 84, se un responsabile del trattamento viola il presente regolamento, determinando le finalità e i mezzi del trattamento, è considerato un titolare del trattamento in questione".

L'Interessato: è la persona fisica cui si riferiscono i dati personali oggetto di trattamento.

Il Designato o Autorizzato: è il soggetto persona fisica che effettua materialmente le operazioni di trattamento sui dati personali. L'Autorizzato può operare alle dipendenze del Titolare, ma anche del Responsabile se nominato.

- **Trattamento dei dati:** come descritto dal Garante, è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali. Nello specifico si la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione, così come disposto dall'art. 4 GDRP comma 2 *"«trattamento»: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a*

disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione";

- **Il Rischio:** la probabilità che da un pericolo si produca un danno a cose o persone. Il rischio è lo scenario descrittivo di un evento al quale sono collegate delle conseguenze, definite in termini di gravità e probabilità, legate al trattamento dei dati personali. Il danno prodotto ha come effetto la compressione dei diritti dell'interessato;

- **DPIA:** *Data Protection Impact Assessment* è la Valutazione d'Impatto sulla protezione dei dati);

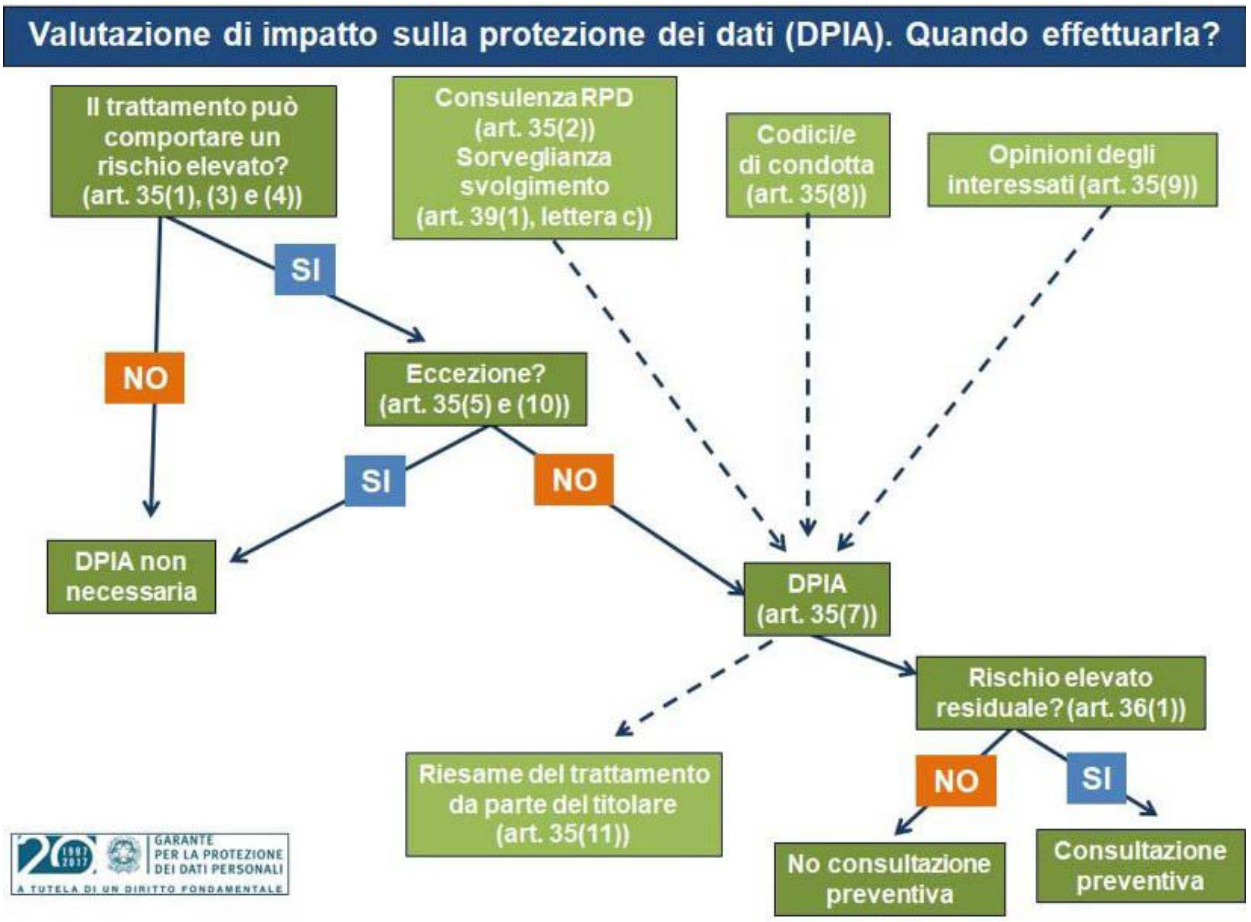
- **GDPR:** *General Data Protection Regulation* è il Regolamento (UE) 2016/679 del 27 aprile 2016;

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La valutazione d'impatto del trattamento (DPIA), cioè *Data Protection Impact Assessment* è un processo volto a descrivere il trattamento dei dati personali, posto in essere, nel caso di specie, attraverso dispositivi di videosorveglianza e sistemi di ausilio alle attività di Polizia Locale descritti dettagliatamente nella Relazione Tecnica Operativa allegata. Questa intende fornire contesto, informazioni tecniche e di sicurezza adottate dal Comune di Oristano per l'acquisizione, il trattamento e l'utilizzo dei dati personali che avviene attraverso il monitoraggio, mediante il sistema di videosorveglianza e i sistemi connessi alle attività effettuate dalla Polizia Locale.

La DPIA, come detto, risulta essenziale e necessaria soltanto quando la tipologia di trattamento, come quello effettuato attraverso la videosorveglianza, "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

Ciò si desume anche dalla immagine riassuntiva, predisposta dal Garante della Privacy, che di seguito descrive quanto detto:



L'OBBLIGATORIETÀ' DELLA DPIA

Ai sensi dell'art. 35 del Regolamento 2016/679 la valutazione d'impatto è obbligatoria nei casi in cui un trattamento può presentare rischi elevati per le persone fisiche, ossia quando:

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.

Inoltre, come definito nel Provvedimento n. 467 del 11 Ottobre 2018 e dettagliato nel suo allegato, il Garante per la Protezione dei Dati Personali ha indicato l'" *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,* tra i quali al punto 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 nn. 3, 7 e 8)"* riconducibili a quelli oggetto di valutazione della presente DPIA.

Quindi, le attività di videosorveglianza effettuate dal Comune di Oristano, per tramite degli impianti gestiti dalla Polizia Locale dello stesso Comune, rientrano nei casi sopra descritti quali trattamenti di dati ad alto rischio.

A questa tipologia di trattamento di dati personali se ne aggiungono altri che, se considerati singolarmente ed autonomamente non necessitano di valutazione del rischio, ma poiché sono effettuati dalla Polizia Locale, in concreto congiuntamente o parallelamente a quelli sopra descritti, il Comune di Oristano ha ritenuto di effettuare la stessa valutazione applicando gli stessi parametri di misurazione.

REVISIONE DELLA DPIA

Secondo il principio della *Privacy By Design* e *Privacy By Default*, gli impianti di videosorveglianza urbana Comunale vanno progettati e resi operativi tenendo presente l'obiettivo della tutela della Privacy e della riduzione dell'impatto che questi possano avere sui diritti e le libertà delle persone fisiche.

A maggior ragione, questo obiettivo deve essere perseguito quando i trattamenti di dati sono potenzialmente ad alto rischio.

In riferimento alla durata di validità del presente atto, occorre precisare che, in via generale, l'aggiornamento è necessario, sia nel rispetto del principio di *Accountability* (art. 24 par. 1 GDPR), sia di tutte le misure di protezione dei dati personali, e va eseguito quindi regolarmente, attraverso la verifica della sicurezza del trattamento e l'eventuale adeguamento delle conseguenti misure di mitigazione del rischio anche per i trattamenti esclusi dal GDPR (art. 15 d. lgs. 51/2018). In particolare, l'aggiornamento della valutazione d'impatto sulla protezione dei dati va effettuato per verificare se insorgano variazioni del rischio (art. 35 par. 11 GDPR). Questo vale anche per le finalità di prevenzione, indagine, accertamento e perseguimento di reati o di esecuzione di sanzioni penali e per la salvaguardia della sicurezza pubblica.

Per questo motivo, la valutazione d'impatto sulla protezione dei dati, è strutturata in maniera tale che sia soggetta a continua revisione e aggiornamento.

CONTENUTI DELLA VALUTAZIONE D'IMPATTO

La DPIA deve contenere, oltre la complessiva valutazione del trattamento dei dati riguardante libertà e diritti delle persone fisiche, alcune parti ritenute inderogabilmente essenziali (art. 35 par. 7 GDPR, art. 23 c. 2, D. Lgs. 51/2018):

- Descrizione generale del trattamento complessivo, contenente la descrizione del trattamento complessivo e delle singole procedure che lo compongono, delle finalità e, quando possibile, l'esplicazione degli interessi legittimi perseguiti dal titolare (art. 35 par. 7 lett. A GDPR, art. 23 c. 2, D. Lgs. 51/2018);
- Valutazione della proporzionalità, di tutti i singoli trattamenti valutati in relazione alle loro finalità (art. 35 par. 7 lett. b GDPR).
- Analisi del Rischio (cd. Risk Analysis), cioè una valutazione dettagliata dei rischi derivanti dal trattamento che possano sui diritti e sulle libertà degli interessati (art. 35 par. 7 lett. c GDPR55, art. 23 c. 2, D. Lgs. 51/2018);
- Mitigazione del Rischio, cioè il progetto contenente nel dettaglio le misure di sicurezza predisposte per minimizzare i rischi sulla sicurezza dei dati personali nel modo più efficace, in conformità al Regolamento Europeo (art. 35 par. 7 lett. d GDPR, art. 23 c. 2, D. Lgs. 51/2018).

Come detto, l'attuale normativa europea per la protezione dei dati assegna al titolare del trattamento l'obbligo di svolgere la valutazione d'impatto Privacy nei casi nei quali, l'utilizzazione di nuove tecnologie nei trattamenti dei dati possano presentare rischi per i diritti e le libertà delle persone fisiche, o in casi specifici, come per la videosorveglianza, ma non definisce le modalità e le tecniche di svolgimento, né tantomeno i parametri per la misurazione del rischio.

Questo, però, non determina che il titolare del trattamento possa limitarsi al mero adempimento formale. Quest'ultimo deve adempiere, infatti, all'obbligo della Valutazione d'impatto sulla protezione dei dati personali nel rispetto del principio di *Accountability*. La responsabilizzazione e l'obbligo di rendicontazione grava sul titolare e dà la misura della correttezza del trattamento eseguito (art. 24 par. 1 GDPR), come l'adozione di misure efficaci per la protezione dei dati personali.

A corollario di questo principio si devono seguire quelli di privacy by design (art. 25 par. 1 GDPR e art. 16 c. 1 D. Lgs. 51/2018) e privacy by default (art. 25 par. 2 GDPR61 e art. 16 c. 2, D. Lgs. 51/201862).

Alla luce di questo, nella stesura della presente DPIA, per assolvere correttamente agli obblighi imposti per la valutazione d'impatto si è effettuata:

- l'analisi dell'impatto dei trattamenti sulle libertà e sui diritti degli interessati, utilizzando metodi standardizzati a livello internazionale e non semplicemente utilizzando dei programmi informatici o delle procedure finalizzate alla mera compilazione formale;
- misurando il rischio in maniera oggettiva e riscontrabile;
- individuando misure specifiche e adattate ai singoli casi per attenuare i rischi;

Per eseguire in maniera oggettiva e dimostrabile quanto richiesto dal Regolamento Europeo si è fatto riferimento alle procedure scientifiche validate a livello internazionale dettate dall'ISO International Organization for Standardization.

ALGORITMO DI VALUTAZIONE

Per comprendere il processo valutativo che porta alla relazione d'impatto DPIA, occorre descrivere alcuni concetti base del **cd. *Risk Management***. A tal riguardo, ci si riferisce all'insieme di attività e processi che un Ente individua, analizza, quantifica, riduce o elimina da un determinato trattamento di dati.

Il *Risk Management* è un processo organizzativo continuo, che deve essere definito da esperti e portato avanti da tutti i dipendenti, in ogni processo al quale le misure sono riferite.

Il Comune di Oristano ritiene di redigere una valutazione di impatto sulla protezione dei dati personali alla luce dei rischi potenziali per i diritti e libertà di tutte le persone coinvolte nel trattamento di dati, effettuati con i sistemi di videosorveglianza e rispetto ai trattamenti connessi alle attività di Polizia Locale.

Lo scopo della valutazione è quello di descrivere tutti gli elementi utili a prendere le decisioni necessarie e a scegliere come mitigare o eliminare il rischio derivante da questo tipo di trattamento dei dati.

I processi di *Risk Management* sono solitamente composti da 6 fasi, ma, secondo la norma ISO 31000 queste si riducono a 4 e si ripetono sistematicamente in modo circolare.
Le 6 fasi del processo di Risk Management sono:

1. Identificazione del rischio;
2. Analisi delle priorità;
3. Pianificazione dell'azione;
4. Monitoraggio;
5. Controllo sistematico del rischio;
6. Apprendimento

Le 4 fasi del Risk Management, come da normativa UNI EN ISO 31000, vanno anch'esse, sovrapponendosi alle precedenti, a fotografare un insieme di azioni e attività messe in atto dall'Ente Pubblico per identificare i rischi e portare avanti le strategie, al fine di poterli mitigare e controllare e continuare a generare valore.
Le 4 fasi sono:

1. **Individuazione del Rischio** (UNI EN ISO 31000). La prima fase è l'individuazione e la catalogazione dei rischi, descrivendoli qualitativamente in un report dei rischi;
2. **Quantificazione del Rischio**. In questa fase di analisi del rischio si valutano i singoli rischi, rispetto alla probabilità che essi si concretizzino (*likehood*) e conseguenze derivate. L'analisi del rischio è volta a verificare la probabilità che si verifichino anche i cd. *rischi correlati tra loro o sovrapposti*, secondo una valutazione volta a definire le conseguenze dell'aggregazione del rischio.
3. **Valutazione del rischio**. La valutazione del rischio descrive tutte le attività che l'Ente vuole predisporre per contrastare tutti i rischi individuati. Il Comune di Oristano ha adottato una serie di attività attive preventive secondo i principi di *Privacy By Design* e *Privacy By Default* riducendo la possibilità che si verifichi un rischio.
   Anche dopo aver adottato tutte le misure di mitigazione, permane sempre un rischio residuale che espone l'Ente al pericolo derivante da queste attività.
4. **Controllo del rischio**. Con il controllo del rischio si verifica l'efficacia delle misure di minimizzazione del rischio adottate.

CONCLUSIONI

Sulla base delle valutazioni sopra descritte e degli allegati al presente documento e ivi elencati, il sottoscritto Dirigente Comandante pro tempore del Corpo di Polizia Locale del Comune di Oristano, delegato dal Sindaco allo svolgimento dei compiti in qualità di titolare, nonché designato con compiti e funzioni specifiche per il trattamento dati riguardante la videosorveglianza e del trattamento dati connesso alle funzioni di Polizia Locale, con il supporto di personale dipendente dell'Ente, che ha prodotto una relazione Tecnica Ingegneristica Preliminare Alla Valutazione Di Impatto (DPIA), relativa allo "*Studio ed analisi dell'impianto di videosorveglianza esistente con particolare attenzione alle possibili criticità legate all'accesso ai dati e alle caratteristiche della infrastruttura di rete*" e "*Studio e analisi dei software e dell'hardware della Centrale Operativa*", con l'ausilio di un consulente per la formazione specifica in materia di Privacy e Videosorveglianza e redazione di DPIA, ha redatto la presente DPIA.

Risultato complessivo della valutazione derivato dalla media ponderata tra tutte le schede di valutazione sopra elencate e descritte:

VALUTAZIONE DEL LIVELLO DI RISCHIO
BASSO

Di conseguenza si ritiene, allo stato attuale, non sussista un rischio elevato per i diritti e le libertà delle persone e di conseguenza non è richiesta una consultazione preventiva all'Autorità Garante.

Oristano, __/___/_____

Il Dirigente Comandante della Polizia Locale

Firmato digitalmente da:
URAS GIOVANNI NICOLA
Firmato il 17/12/2024 10:36
Seriale Certificato: 1591442
Valido dal 01/07/2022 al 01/07/2025
InfoCamere Qualified Electronic Signature CA

ALLEGATI