E. I.

Città di Modica

DELIBERAZIONE
della
GIUNTA COMUNALE
N. 112 del 9.4.2021

OGGETTO: Approvazione valutazione d'impatto sulla protezione dei dati personali (D.P.I.A.) acquisiti tramite il sistema di videosorveglianza installato nel territorio del Comune di Modica.

L'anno duemilaventuno il giorno NOVE del mese di APRILE alle ore 16,10 nel Palazzo di Città e nella stanza del Sindaco, in seguito ad invito di convocazione, si è riunita la Giunta Comunale, alla quale risultano presenti:

		Presente	Assente
Abbate Ignazio	Sindaco	X	
Viola Rosario	Vice Sindaco	X	
Aiello Anna Maria	Assessore	X	
Linguanti Giorgio	Assessore	X	
Lorefice Salvatore Pietro	Assessore	X	
Monisteri Caschetto Maria	Assessore	X	
Belluardo Giorgio	Assessore	X	

Partecipa il Segretario Generale, Dott. Giampiero Bella, con funzioni consultive, referenti, di assistenza e verbalizzazione, ai sensi dell'art.97, comma 4, lett. a) del d. Lgs. n.267/2000.

Assunta la presidenza, il Sindaco, Ignazio Abbate, constatata la legalità dell'adunanza, dichiara aperta la seduta ed invita la Giunta Comunale all'esame della proposta di deliberazione in oggetto, in merito alla quale sono stati espressi i pareri di legge.

LA GIUNTA COMUNALE

Esaminata l'allegata proposta di deliberazione di pari oggetto, prot. n. 16668 del 09.04.2021, parte integrante e sostanziale del presente atto;

Considerato che della stessa se ne condividono tutti i presupposti di fatto e di diritto;

Preso atto che su tale proposta di deliberazione è stato espresso il parere favorevole in ordine alla regolarità tecnica dello stesso proponente, ai sensi dell'art. 1, comma 1, lett.i, della L.R. n. 48/91, come modificato ed integrato dall'art.12 L.R. n.30/2000, e che la stessa non necessita di ulteriori pareri;

Ritenuto di provvedere in merito;

Visto lo Statuto Comunale;

Visto il vigente O.R.E.L.;

Vista la L.R. n. 48/1991 e successive modifiche ed integrazioni;

Visto l'art. 12 della L.R. n. 44/1991;

Ad unanimità di voti, resi nelle forme di legge

DELIBERA

1. Di approvare e far propria la proposta di deliberazione di pari oggetto richiamata in premessa, che si allega alla presente deliberazione per farne parte integrante e sostanziale;

2. Di dichiarare la presente deliberazione immediatamente esecutiva, con successiva e separata votazione unanime, resa ai sensi dell'art. 12, comma 2, della L.R. n. 44/91, attesa l'urgenza di provvedere in merito, nell'interesse dell'Ente, per i motivi citati nella stessa proposta deliberativa.

E. I.

Città di Modica

PROPOSTA di DELIBERAZIONE
della GIUNTA COMUNALE

SETTORE VIII
Polizia Locale

Prot. n. 16668 del 29 APR 2021

OGGETTO: Approvazione Valutazione D'impatto Sulla Protezione dei Dati Personali (D.P.I.A.) acquisiti tramite il sistema di videosorveglianza installato nel territorio del Comune di Modica.

Il sottoscritto Cannizzaro Rosario – Responsabile P.O. VIII Settore - propone il seguente schema di deliberazione:

Visto il Regolamento UE 2016/679 (GDPR – General Data Protection Regulation) relativo alla "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati";

Richiamato in particolare l'art. 35 del predetto Regolamento *"Valutazione d'impatto sulla protezione dei dati"* o D.P.I.A. (*Data Protection Impact Assessment),* relativo all'adempimento, in capo al titolare del trattamento, della procedura che analizza preventivamente l'intero processo di trattamento dei dati allorché tale processo preveda l'uso di nuove tecnologie e presenti un rischio elevato per i diritti e le libertà delle persone fisiche interessate;

Preso atto che:

- la procedura di *"valutazione"* è prescritta nei casi indicati dal comma 3 del citato art. 35 ed in particolare nei casi di sorveglianza sistematica, su larga scala, di una zona accessibile al pubblico;
- il Garante per la protezione dei dati personali si è espresso sulla Valutazione d'impatto, con delibera n.467/2018, fornendo un elenco non esaustivo di trattamenti rischiosi per cui è necessaria la valutazione fra i quali vi rientra l'ipotesi di "utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati", di "dati aventi carattere estremamente personale", di "uso di tecnologie evolute";
- trattandosi di una valutazione preventiva dovrà prevedere le misure da adottare a garanzia di un corretto trattamento dei dati;

Riscontrato, in base alla predetta disciplina, che il trattamento di dati personali effettuato tramite sistemi di videosorveglianza necessita della valutazione d'impatto, poiché rientra nel caso previsto all'art. 35 comma 3 lett. c) del GDPR;

Rilevato altresì dal comma 2 del citato art. 35 che 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;

Considerato che, ai sensi dell'art. 2 del Regolamento comunale attuativo del Regolamento UE 2016/679 in materia di protezione dati personali, adottato con Delibera di Consiglio Comunale n. 51/2018, il Comune di Modica, rappresentato ai fini previsti dal GDPR dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti in banche dati e quindi anche dei dati acquisiti mediante l'impianto di videosorveglianza;

Richiamata la determina n.2693/2020 con la quale è stato nominato Responsabile per la Protezione Dati (D.P.O), per il Comune di Modica, il Gruppo Consulting Soc. Coop STP con sede a Ragusa in Via Mons. G. Iacono, n.20, legale rappresentante Ing. Carmelo Mezzasalma;

Preso atto che uno dei compiti fondamentali posto in capo al D.P.O. è quello previsto dalla lettera c) dell'art. 39 del GDPR, ossia fornire, a richiesta, parere sulla valutazione d'impatto e sorvegliare altresì lo svolgimento della relativa procedura;

Vista la allegata Valutazione d'impatto o DPIA, assunta al prot. n. 15623 del 02/04/2021, avente ad oggetto "*Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679) Polizia Locale del Comune di Modica – Sistema di videosorveglianza*", formulata con la consulenza del Responsabile Protezione Dati, come sopra indicato, e corredata da "validazione" dello stesso;

Verificate le risultanze della predetta DPIA dalle quali si evince che il trattamento dei dati in oggetto presenta una probabilità di rischio "*limitata*" per cui non si rende necessario la consultazione preventiva del Garante per la protezione dei dati personali (Art. 9 Regolamento comunale);

Dato atto comunque che la Valutazione d'impatto o DPIA costituisce un documento suscettibile di continuo aggiornamento in particolare quando insorgono variazioni del rischio per l'introduzione di nuove tecnologie o in relazione a nuove criticità;

Ritenuto necessario procedere alla approvazione dell'allegato documento di Valutazione d'impatto o DPIA, parte integrante e sostanziale del presente atto;

Visto il D. Lgs. 18 agosto 2000, n.267;

Vista la L.R. n. 48/1991 e ss.mm.ii.;

Visto l'art. 12, comma 2, della L.R. n. 44/1991;

PROPONE

1. di approvare l'allegato documento di Valutazione d'impatto o DPIA avente ad oggetto "*Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679) Polizia Locale del Comune di Modica – Sistema di videosorveglianza*", parte integrante e sostanziale del presente atto;

2. di trasmettere il presente atto al Responsabile P.O. del Settore VIII - Polizia Locale;

3. di disporre la pubblicazione del presente provvedimento sul sito web dell'Ente – Sezione Atti – "Protezione Dati Regolamento UE 679/2016" – sottosezione Settore VIII - Atti Videosorveglianza Polizia Locale - a cura del Responsabile del sito internet dell'Ente al quale il provvedimento dovrà essere trasmesso;

4. di dichiarare, con separata ed unanime votazione, il presente atto immediatamente esecutivo ai sensi dell'art. 12 comma 2 della Legge regionale n. 44/91.

Il Responsabile P.O. VIII Settore
Rosario Cannizzaro

Sulla proposta di deliberazione di cui sopra sono stati espressi i seguenti pareri, ai sensi dell'art. 1, comma 1, lett. i, L.R. n. 48/91, come modificato ed integrato dall'art. 12 L.R. n.30/2000.

Parere del Responsabile del Settore proponente per la regolarità tecnica: **favorevole /sfavorevole** Modica, lì 09-04-2021 **Il Responsabile del Settore**
Parere del Responsabile del settore finanziario per la regolarità contabile: **favorevole /sfavorevole** Modica, lì **Il Responsabile del Settore Finanziario**
Per l'assunzione dell'impegno di spesa, si attesta la regolare copertura finanziaria, ai sensi degli artt. 153, 183, 191 del D.L.vo n.267/2000, con spesa da impegnare al cap. _____ del Bilancio ..... Modica, lì **Il Responsabile del Settore Finanziario**

La proposta infra riportata si compone di n. _____ pagine, incluso il presente prospetto,.

Il Responsabile proponente

Visto
L'Assessore al ramo

La presente proposta è approvata con deliberazione della Giunta Municipale n. 112 del 9/4/2021

IL SEGRETARIO GENERALE
Dr. Giampiero Bella

e.belviglio

15623

02 APR. 2021

Da "gruppoconsulting" <gruppoconsulting@pec.it>
A "comandopm.comune.modica@pec.it" <comandopm.comune.modica@pec.it>
Cc "Carmelo Mezzasalma" <carmelo@mtplan.it>, "bracchitta@privacyworld.it" <bracchitta@privacyworld.it>
Data venerdì 2 aprile 2021 - 10:20

Invio Valutazione di impatto privacy

GRUPPO CONSULTING

Via Mons Iacono n°20
97100 RAGUSA
Telefax 0932642435 - 0932257584
http://www.gruppoconsulting.it

Alla c.a. del Signor Sindaco del Comune di Modica
e del Comandante della Polizia Municipale

In relazione all'attività di videosorveglianza, per quanto di competenza si invia in allegato Valutazione di impatto privacy.

Distinti saluti
Il Presidente del CdA
Carmelo Mezzasalma

Allegato(i)

DPIA_polizialocale_vs.pdf (441 KB)

Valutazione d'impatto sulla protezione dei dati (Art. 35 GDPR 2016/679)
Polizia Locale del Comune di Modica
Sistema di videosorveglianza

Valutazione d'impatto sulla protezione dei dati (Data Protection Impact Assessment - DPIA) alla luce delle linee guida del WP Art. 29 del 4.10.2017 e del Decreto Legislativo N.101 del 10 Agosto 2018 (Modifica del Codice Privacy D. Lgs. n. 101/2018)

Premessa La disciplina sulla DPIA contenuta nel GDPR deve essere integrata da quanto specificato dal WP art. 29 nelle linee guida pubblicate in data 4.10.2017 (versione definitiva). In particolare, il WP art. 29 ha definito i criteri in base ai quali decidere se fare ricorso o meno a una DPIA, quali sono le metodologie utilizzabili dai titolari per condurre una DPIA e quali sono gli elementi sufficienti per una DPIA accettabile.

1. Soggetto obbligato

Il GDPR impone al solo **titolare** del trattamento di effettuare la DPIA, qualora ne ricorrano i presupposti (cfr. art. 35). Nello svolgimento di una DPIA il titolare potrà essere coadiuvato dal DPO e dal responsabile. Quando un trattamento è svolto in **contitolarità**, nella DPIA devono essere specificati con precisione gli obblighi che incombono su ciascun titolare, ad esempio con riferimento alla responsabilità delle singole misure finalizzate alla gestione dei rischi.

2. In quali casi è necessario effettuare una DPIA

La DPIA è obbligatoria solo qualora un trattamento "possa presentare un **rischio elevato**" per i diritti e le libertà delle persone fisiche. Nei **casi dubbi**, si raccomanda di svolgere comunque una DPIA, in quanto questa è una procedura che permette di realizzare e dimostrare la conformità con le norme del GDPR. Il riferimento ai "**diritti e alle libertà**" va inteso come relativo al diritto alla privacy e anche ad altri diritti fondamentali, quali la libertà di espressione e di pensiero, la libertà di movimento, il divieto di discriminazioni, il diritto alla libertà di coscienza e di religione.

2.a) Casi previsti dal GDPR

L'art. 35, paragrafo 3, GDPR cita espressamente tre casi in cui sussiste un rischio elevato ed è quindi necessaria l'effettuazione di una DPIA, ossia: **a)** valutazione sistematica e globale, basata su un trattamento automatizzato, degli aspetti personali relativi a persone fisiche (compresa la **profilazione**), e sulla quale si fondano decisioni che hanno effetti giuridici o incidono significativamente su tali soggetti;

b) trattamento su **larga scala** di **dati sensibili o giudiziari;**

c) sorveglianza sistematica su **larga scala** di una **zona accessibile al pubblico.** Tale elenco non è esaustivo. Secondo il WP art. 29 la DPIA deve essere anche condotta per valutare l'**impatto di un nuovo dispositivo tecnologico** in termini di protezione dei dati. Il GDPR assegna alle autorità di controllo (per l'Italia, al Garante) il compito di redigere e rendere pubblico **un elenco delle tipologie di trattamento** da assoggettare e da non assoggettare a DPIA (cfr. art. 35, paragrafi 4 e 5).

2.b) I 9 criteri enunciati dal WP art. 29

Secondo il WP art. 29 i seguenti **9 criteri** devono essere presi in esame sia dalle autorità di controllo per redigere l'elenco delle tipologie di trattamento da assoggettare a DPIA *ex* art. 35, par. 4, GDPR, sia dai titolari per comprendere quando siano tenuti a svolgere una DPIA:

1. trattamenti valutativi o di *scoring,* compresa la **profilazione** e attività predittive, in particolare a partire da "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" (considerando 71 e 91). Ad es.: società che crea profili comportamentali o di *marketing* a partire dalla operazioni o dalla navigazione compiute sul proprio sito internet;
2. decisioni automatizzate che producono significativi effetti giuridici o di analoga natura. Ad es.: trattamento che possa comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione;
3. monitoraggio sistematico: trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o "la sorveglianza sistematica di un'area accessibile al pubblico"; **4. dati sensibili o dati di natura estremamente personale:** si tratta dei dati sensibili di cui all'art. 9 e dei dati giudiziari di cui all'art. 10;

5. trattamenti di dati su larga scala: il GDPR si occupa del termine "larga scala" nel considerando 91. Il Gruppo art. 29 raccomanda di tenere conto dei seguenti fattori al fine di stabile se un trattamento sia svolto su larga scala:

a) numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento;

b) volume dei dati e/ o ambito delle diverse tipologie di dati oggetto di trattamento;

c) durata, o persistenza, dell'attività di trattamento;

d) ambito geografico dell'attività di trattamento;

6. combinazione o raffronto di insieme di dati, per esempio derivanti da due o più trattamenti svolti per diverse finalità e/ o da titolari distinti;

7. dati relativi a interessati vulnerabili (cons. 75), compresi i minori, i dipendenti, i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti e ogni interessato rispetto al quale possa identificarsi una situazione di disequilibrio con il rispettivo titolare del trattamento;

8. utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

9. trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (art. 22 e cons. 91). Ad es.: *screening* dei clienti di una banca attraverso i dati registrati in una centrale rischi al fine di stabilire se ammetterli o meno ad un finanziamento.

Quando ricorrono almeno **due dei criteri** sopra indicati, il titolare dovrà condurre una DPIA. Tuttavia, in alcuni casi si dovrà procedere a una DPIA anche di fronte ad un trattamento che soddisfi **solo uno dei criteri** di cui sopra. È, inoltre, possibile che vi sia perfetta coincidenza tra le ipotesi legislative e i criteri enucleati dal WP art. 29 (ad es. la profilazione sistematica che impatta significativamente sull'interessato non è solo un caso legislativamente previsto di DPIA obbligatoria *ex* art. 35, par. 3, lett. a) GDPR, ma anche la combinazione dei criteri n° 1, 2 e 3 stabiliti dal WP art. 29). Si potrebbe verificare anche il caso, ma il WP art. 29 non chiarisce quando tale ipotesi potrebbe verificarsi in concreto, in cui il titolare esclude che debba svolgersi una DPIA perché, pur in presenza dei criteri summenzionati, il trattamento **non** presenta un rischio elevato. In questo caso, il titolare dovrà motivare e documentare la scelta della mancata conduzione della DPIA, allegando o annotando il parere del **DPO.** Possiamo immaginare che si tratti della situazione in cui vengano adottate dal titolare misure di sicurezza tali da scongiurare la possibilità di rischio (elevato) per i diritti e le libertà degli interessati (ad es. mediante la pseudonimizzazione e la cifratura dei dati che vengono profilati).
Di seguito si riportano alcuni esempi di trattamento e di funzionamento operativo dei criteri fissati dal WP art. 29:
Esempi di trattamento: azienda che controlla sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su internet, ecc. **~criteri pertinenti:** monitoraggio sistematico; dati relativi a interessati vulnerabili; **obbligo di DPIA probabile.**

Esempi di trattamento: raccolta di dati pubblici tratti dai *social media* per la creazione di profili **~criteri pertinenti:** valutazione o *scoring;* dati trattati su larga scala; raffronto o combinazione di insiemi di dati; dati sensibili o dati di natura estremamente personale; **obbligo di DPIA probabile.**

Esempi di trattamento: rivista *online* che utilizza una *mailing list* per inviare agli abbonati un bollettino giornaliero di carattere generale ~**criteri pertinenti:** dati trattati su larga scala; **obbligo di DPIA non probabile.**

Esempi di trattamento: sito di *e-commerce* che pubblicizza parti di ricambio per auto d'epoca con limitata profilazione riferita ad alcune sezioni del sito e basata su pregressi acquisti effettuati ~**criteri pertinenti:** valutazione o *scoring*, **obbligo di DPIA non probabile.**

Per quanto riguarda l'aspetto legislativo, le modifiche introdotte dal D. Lgs. n. 101/2018 indicate di seguito delimitano lo spazio di svolgimento dell'attività di trattamento.

Titolo VI - Istruzione

Capo I - Profili generali

Art. 96 ***(Trattamento di dati relativi a studenti)*** 1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché' le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 1 O del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità. 2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

Titolo VII - *Trattamenti* a *fini di archiviazione nel pubblico interesse, di ricerca scientifica* o *storica* o a *fini statistici*

Capo I - Profili generali

Art. 97 ***(Ambito applicativo)***

1. Il presente titolo disciplina il trattamento dei dati personali effettuato a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, ai sensi dell'articolo 89 del regolamento.

Art. 98 - Finalità di rilevante interesse pubblico (abrogato)

Art. 99 ***(Durata del trattamento)***

1. Il trattamento di dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici può essere effettuato anche oltre il periodo di tempo necessario per conseguire i diversi scopi per i quali i dati sono stati in precedenza raccolti o trattati.

2. A fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici possono comunque essere conservati o ceduti ad altro titolare i dati personali dei quali, per qualsiasi causa, è cessato il trattamento nel rispetto di quanto previsto dall'articolo 89, paragrafo 1, del Regolamento.

Art. 100 - Dati relativi ad attività di studio e ricerca

1. Al fine di promuovere e sostenere la ricerca e la collaborazione in campo scientifico e tecnologico i soggetti pubblici, ivi comprese le università e gli enti di ricerca, possono con autonome determinazioni comunicare e diffondere, anche a privati e per via telematica, dati relativi ad attività di studio e di ricerca, a laureati, dottori di ricerca, tecnici e tecnologi, ricercatori, docenti, esperti e studiosi, con esclusione di quelli di cui agli articoli 9 e 1 O del Regolamento.

2. Resta fermo il diritto dell'interessato di rettifica, cancellazione, limitazione e opposizione ai sensi degli articoli 16, 17, 18 e 21 del Regolamento.

3. I dati di cui al presente articolo non costituiscono documenti amministrativi ai sensi della Legge 7 agosto 1990, n. 241.
4. I dati di cui al presente articolo possono essere successivamente trattati per i soli scopi in base ai quali sono comunicati o diffusi.

4-bis. I diritti di cui al comma 2 si esercitano con le modalità previste dalle regole deontologiche.

Capo II - *Trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica*

Art. 101 - Modalità di trattamento

1. I dati personali raccolti a fini di archiviazione nel pubblico interesse o di ricerca storica non possono essere utilizzati per adottare atti o provvedimenti amministrativi sfavorevoli all'interessato, salvo che siano utilizzati anche per altre finalità nel rispetto dell'articolo 5 del regolamento.
2. I documenti contenenti dati personali, trattati a fini di archiviazione nel pubblico interesse o di ricerca storica, possono essere utilizzati, tenendo conto della loro natura, solo se pertinenti e indispensabili per il perseguimento di tali scopi. I dati personali diffusi possono essere utilizzati solo per il perseguimento dei medesimi scopi.
3. I dati personali possono essere comunque diffusi quando sono relativi a circostanze o fatti resi noti direttamente dall'interessato o attraverso suoi comportamenti in pubblico.

Art. 102 - *Regole deontologiche per il trattamento a fini di archiviazione nel pubblico interesse o di ricerca storica*

1. Il Garante promuove, ai sensi dell'articolo *2-quater,* la sottoscrizione di regole deontologiche per i soggetti pubblici e privati, ivi comprese le società scientifiche e le associazioni professionali, interessati al trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica.
2. Le regole deontologiche di cui al comma 1 individuano garanzie adeguate per i diritti e le libertà dell'interessato in particolare: a. le regole di correttezza e di non discriminazione nei confronti degli utenti da osservare anche nella comunicazione e diffusione dei dati, in armonia con le disposizioni del presente codice e del Regolamento applicabili ai trattamenti di dati per finalità giornalistiche o di pubblicazione di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica; b. le particolari cautele per la raccolta, la consultazione e la diffusione di documenti concernenti dati idonei a rivelare lo stato di salute, la vita sessuale o rapporti riservati di tipo familiare, identificando casi in cui l'interessato o chi vi abbia interesse è informato dall'utente della prevista diffusione di dati; c. le modalità di applicazione agli archivi privati della disciplina dettata in materia di trattamento dei dati a fini di archiviazione nel pubblico interesse o di ricerca storica, anche in riferimento all'uniformità dei criteri da seguire per la consultazione e alle cautele da osservare nella comunicazione e nella diffusione.

Art. 103 - *Consultazione di documenti conservati in archivi*

1. La consultazione dei documenti conservati negli archivi di Stato, in quelli storici degli enti pubblici e in archivi privati dichiarati di interesse storico particolarmente importante è disciplinata dal decreto legislativo 22 gennaio 2004, n. 42 e dalle relative regole deontologiche.

TITOLO VIII - *Trattamenti nell'ambito del rapporto di lavoro*

Capo I - Profili generali

Art. 111 *(Regole deontologiche per trattamenti nell'ambito del rapporto di lavoro)*

1. Il Garante promuove, ai sensi dell'articolo *2-quater,* l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato.
2. **Art. 111-bis *(Informazioni in caso di ricezione di curriculum)***
3. 1. Le informazioni di cui all'articolo 13 del Regolamento, nei casi di ricezione dei *curricula* spontaneamente trasmessi dagli interessati al fine della instaurazione di un rapporto di lavoro, vengono fornite al momento del primo contatto utile, successivo all'invio del *curriculum* medesimo. Nei limiti delle finalità di cui all'articolo 6, paragrafo 1, lettera b), del Regolamento, il consenso al trattamento dei dati personali presenti nei *curricu/a* non è dovuto.
4. **Art. 112 - Finalità di rilevante interesse pubblico (abrogato)**

Capo II - *Trattamento di dati riguardanti i prestatori di lavoro*

5. **Art. 113 Raccolta di dati e pertinenza**

1. Resta fermo quanto disposto dall'articolo 8 della legge 20 maggio 1970, n.300 nonché dall'articolo 1 O del decreto legislativo 1 O settembre 2003, n. 276. **Capo lii - *Controllo a distanza, lavoro agile* e *telelavoro***

6. **Art. 114** ***(Garanzie in materia di controllo a distanza)***
   1. Resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300.
7. **Art. 115** ***(Telelavoro, lavoro agile* e *lavoro domestico)***
   1. Nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale.
   2. il lavoratore domestico è tenuto a mantenere la necessaria riservatezza per tutto quanto si riferisce alla vita familiare.

Capo IV - Istituti di patronato e di assistenza sociale

8. **Art. 116 Conoscibilità di dati su mandato dell'interessato**
   1. Per lo svolgimento delle proprie attività gli istituti di patronato e di assistenza sociale, nell'ambito del mandato conferito dall'interessato, possono accedere alle banche di dati degli enti eroganti le prestazioni, in relazione a tipi di dati individuati specificamente con il consenso manifestato dall'interessato medesimo.
   2. Il Ministro del lavoro e delle politiche sociali stabilisce con proprio decreto le linee- guida di apposite convenzioni da stipulare tra gli istituti di patronato e di assistenza sociale e gli enti eroganti le prestazioni.

Titolo IX - *Altri trattamenti in ambito pubblico* o *di interesse pubblico* Capo I - *(Assicurazioni)*

Art. 117 - Affidabilità e puntualità nei pagamenti(abrogato) Art. 118 - Informazioni commerciali (abrogato)

Art. 119 - Dati relativi al comportamento debitorio (abrogato)

Art. 120 - Sinistri

1. L'Istituto per la vigilanza sulle assicurazioni definisce con proprio provvedimento le procedure e le modalità di funzionamento della banca di dati dei sinistri istituita per la prevenzione e il contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie per i veicoli a motore immatricolati in Italia, stabilisce le modalità di accesso alle informazioni raccolte dalla banca dati per gli organi giudiziari e per le pubbliche amministrazioni competenti in materia di prevenzione e contrasto di comportamenti fraudolenti nel settore delle assicurazioni obbligatorie, nonché le modalità e i limiti per l'accesso alle informazioni da parte delle imprese di assicurazione.
2. Il trattamento e la comunicazione ai soggetti di cui al comma 1 dei dati personali sono consentiti per lo svolgimento delle funzioni indicate nel medesimo comma.
3. Per quanto non previsto dal presente articolo si applicano le disposizioni dall'articolo 135 del codice delle assicurazioni private di cui al decreto legislativo 7 settembre 2005, n. 209.

Titolo X - Comunicazioni elettroniche

Capo I - Servizi di comunicazione elettronica

Art. 121 (Servizi interessati e definizioni)

1. Le disposizioni del presente titolo si applicano al trattamento dei dati personali connesso alla fornitura di servizi di comunicazione elettronica accessibili al pubblico su reti pubbliche di comunicazioni, comprese quelle che supportano i dispositivi di raccolta dei dati e di identificazione.

1-bis. Ai fini dell'applicazione delle disposizioni del presente titolo si intende per:

a) «comunicazione elettronica», ogni informazione scambiata o trasmessa tra un numero finito di soggetti tramite un servizio di comunicazione elettronica accessibile al pubblico. Sono escluse le informazioni trasmesse al pubblico tramite una rete di comunicazione elettronica, come parte di un servizio di radiodiffusione, salvo che le stesse informazioni siano collegate ad un contraente o utente ricevente, identificato o identificabile;

b) «chiamata», la connessione istituita da un servizio di comunicazione elettronica accessibile al pubblico che consente la comunicazione bidirezionale;

c) «reti di comunicazione elettronica», i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione o di instradamento e altre risorse, inclusi gli elementi di rete non attivi, che consentono di trasmettere segnali via cavo, via radio, a mezzo di fibre ottiche o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri mobili e fisse a commutazione di circuito e a commutazione di pacchetto, compresa Internet, le reti utilizzate per la diffusione circolare dei programmi sonori e televisivi, i sistemi per il trasporto della corrente elettrica, nella misura in cui siano utilizzati per trasmettere i segnali, le reti televisive via cavo, indipendentemente dal tipo di informazione trasportato;

d) «rete pubblica di comunicazioni», una rete di comunicazione elettronica utilizzata interamente o prevalentemente per fornire servizi di comunicazione elettronica accessibili al pubblico, che supporta il trasferimento di informazioni tra i punti terminali di reti;
e) «servizio di comunicazione elettronica», i servizi consistenti esclusivamente o prevalentemente nella trasmissione di segnali su reti di comunicazioni elettroniche, compresi i servizi di telecomunicazioni e i servizi di trasmissione nelle reti utilizzate per la diffusione circolare radiotelevisiva, nei limiti previsti dall'articolo 2, lettera e), della direttiva 2002/21/CE del Parlamento europeo e del Consiglio, del 7 marzo 2002;
f) «contraente», qualunque persona fisica, persona giuridica, ente o associazione parte di un contratto con un fornitore di servizi di comunicazione elettronica accessibili al pubblico per la fornitura di tali servizi, o comunque destinatario di tali servizi tramite schede prepagate;
g) «utente», qualsiasi persona fisica che utilizza un servizio di comunicazione elettronica accessibile al pubblico, per motivi privati o commerciali, senza esservi necessariamente abbonata;
h) «dati relativi al traffico», qualsiasi dato sottoposto a trattamento ai fini della trasmissione di una comunicazione su una rete di comunicazione elettronica o della relativa fatturazione;
i) «dati relativi all'ubicazione», ogni dato trattato in una rete di comunicazione elettronica o da un servizio di comunicazione elettronica che indica la posizione geografica
dell'apparecchiatura terminale dell'utente di un servizio di comunicazione elettronica accessibile al pubblico;
j) «servizio a valore aggiunto», il servizio che richiede il trattamento dei dati relativi al traffico o dei dati relativi all'ubicazione diversi dai dati relativi al traffico, oltre a quanto e' necessario per la trasmissione di una comunicazione o della relativa fatturazione;
k) «posta elettronica», messaggi contenenti testi, voci, suoni o immagini trasmessi attraverso una rete pubblica di comunicazione, che possono essere archiviati in rete o nell'apparecchiatura terminale ricevente, fino a che il ricevente non ne ha preso conoscenza.

Informazioni sulla PIA

Nome della PIA
DPIA Videosorveglianza Polizia Locale

Nome autore
Sindaco

Nome valutatore
Dirigente Polizia Locale

Nome validatore
Responsabile protezione dati Dott. Ing. Carmelo Mezzasalma

Data di creazione
17/03/2021

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Il trattamento operato dagli agenti di Polizia Locale, interamente o parzialmente automatizzato, dei dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza attivati nel territorio dell'Ente, ai sensi del Reg. UE 2016/679, della Direttiva UE 2016/680, in osservanza delle disposizioni contenuti nel "decalogo" del 8 aprile 2010 dal Garante della Privacy e del Codice Nazionale sulla Privacy dlgs 196/2003.

L'impatto è valutato con particolare attenzione ai diritti e alle libertà degli interessati e ha come obbiettivo di verificare e garantire la protezione dei dati personali di tutti coloro che entrano in contatto o in relazione con l'attività di videosorveglianza.

L'utilizzo degli impianti è finalizzato a:

a. Attività di prevenzione, indagine, accertamento e perseguimento di atti delittuosi, attività illecite ed episodi di microcriminalità commessi sul territorio comunale, al fine di garantire maggiore sicurezza ai cittadini nell'ambito del più ampio concetto di "sicurezza urbana" di cui all'articolo 4 del decreto legge n. 14/2017 e s.m.i., delle attribuzioni del Sindaco in qualità di autorità locale di cui all'art. 50 e di ufficiale di governo di cui all'art. 54 comma 4 e 4-bis del d.lgs 267/2000;

b. Prevenire e reprimere ogni tipo di illecito, di natura penale o amministrativa, in particolare legato a fenomeni di degrado, di discarica di materiale e di sostanze pericolose o di abbandono di rifiuti, e svolgere i controlli volti ad accertare le violazioni delle norme contenute nel regolamento di polizia urbana, nei Regolamenti locali in genere e nelle Ordinanze Sindacali;

c. Vigilare sull'integrità, sulla conservazione e sulla tutela del patrimonio pubblico e privato;

d. Tutelare l'ordine, il decoro e la quiete pubblica;

e. Controllare aree specifiche del territorio comunale;

f. Monitorare e controllare la viabilità e i flussi di traffico;

Quali sono le responsabilità connesse al trattamento?

Le responsabilità del trattamento sono connesse ai ruoli ricoperti, il titolare del trattamento è il Sindaco pro tempore, il designato al trattamento (responsabili interni) è il dirigente/responsabile di posizione organizzativa del servizio di Polizia Locale, se formalmente nominato, possono essere nominati come responsabili esterni del trattamento tutti i soggetti fisici o giuridici che gestiscono per conto dell'ente dati personali nell'ambito di un appalto di servizi relativo al supporto per la gestione degli impianti.

Ci sono standard applicabili al trattamento?
Al momento non sono contemplati standard da applicare direttamente al trattamento, tuttavia l'attività di videosorveglianza è disciplinata da specifico regolamento dell'ente.

Valutazione : Accettabile

Dati, processi e risorse di supporto
Quali sono i dati trattati?
Gli impianti riprendono e registrano immagini che permettono di identificare in modo diretto o indiretto le persone riprese, consentono riprese unicamente di video o foto e sono installati nel territorio dell'Ente e possono essere sia fissi che mobili.

Vengono trattati i dati degli autoveicoli, targhe e persone fisiche che circolano in prossimità delle telecamere.

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
Il ciclo di vita dei dati prevede i seguenti trattamenti acquisizione, registrazione, organizzazione, conservazione, consultazione, raffronto o interconnessione, limitazione, pseudonimizzazione. Le immagini sono viste in tempo reale direttamente presso il comando della Polizia locale da persone autorizzate, le immagini rilevanti ogni sorta di infrazione o reato vengono scaricate in locale attraverso dispositivo di memoria di massa e messe a disposizione in caso di necessità agli operatori di giustizia, le immagini e video vengono sovrascritti in maniera automatica dopo sette giorni dalla loro rilevazione.
Quali sono le risorse di supporto ai dati?

Gli impianti consentono riprese video e foto a colori, diurne e notturne, in condizioni di sufficiente illuminazione naturale o artificiale, gli impianti di videosorveglianza sono sempre in funzione e registrano in maniera continuativa.
I segnali video e foto delle unità di ripresa sono inviati presso la sede della Polizia locale su data center individuato appositamente dove sono registrati su appositi server. In queste sedi le immagini sono visualizzate su monitor e hardware client appositamente configurato il cui accesso è protetto, riservato e consentito unicamente al personale formalmente e appositamente incaricato.

Valutazione : Accettabile

Principi Fondamentali

Proporzionalità e necessità
Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento dei dati personali, acquisiti mediante l'utilizzo degli impianti di videosorveglianza gestiti dall'Ente e collegati alle centrali di controllo ubicate presso gli Uffici dell'Ente, si svolge nel rispetto dei diritti, delle libertà fondamentali e della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale.

Garantisce al contempo il rispetto dei diritti delle persone giuridiche e di ogni altro Ente o associazione coinvolti nel trattamento.

L'utilizzo degli impianti comporta esclusivamente il trattamento di dati personali rilevati mediante le riprese video e foto che, in relazione ai luoghi di installazione delle telecamere, interessano i soggetti ed i mezzi di trasporto che transitano nell'area oggetto di sorveglianza.

Valutazione : Accettabile

Quali sono le basi legali che rendono lecito il trattamento?

La base giuridica del trattamento è data dunque dalla necessità di eseguire un compito di interesse pubblico o connesso all'esercizio di pubblici poteri ai sensi dell'art. 6, paragrafo 1, lettera e) GDPR, nonché dal - la necessità di eseguire un compito di un'autorità competente per le finalità di prevenzione, accertamento e perseguimento di reati, salvaguardia contro e la prevenzione di minacce alla sicurezza pubblica ai sensi dell'art. 5 del D.lgs n. 51/2018

Valutazione : Accettabile

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?

In applicazione dei principi di pertinenza, adeguatezza e limitazione dei dati (c.d. minimizzazione dei dati) di cui all'art. 5, Paragrafo 1, lett. c), RGPD, il sistema di videosorveglianza, i sistemi informativi ed i programmi informatici utilizzati, sono configurati per ridurre al minimo l'utilizzazione di dati personali e identificativi in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Pertanto, deve essere escluso ogni uso superfluo, nonché evitati eccessi e ridondanze nei sistemi di videosorveglianza. Inoltre, qualora non sia necessario individuare le persone, i sistemi devono essere configurati, già in origine, in modo da poter impiegare solo i dati anonimi, con riprese di insieme e, il software utilizzato deve preventivamente essere impostato per cancellare periodicamente ed autonomamente i dati registrati.
In attuazione del principio di limitazione e pertinenza, gli impianti di videosorveglianza e i programmi informatici di gestione sono configurati in modo da ridurre al minimo l'uso di dati personali ed identificativi, in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere raggiunte mediante dati anonimi o con modalità che permettano di identificare l'interessato solo in caso di necessità, sono configurati in modo da raccogliere esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese ed evitando, quando non indispensabili, immagini dettagliate, ingrandite o con particolari non rilevanti

L'attività di videosorveglianza raccoglie esclusivamente i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando quando non indispensabili immagini dettagliate, ingrandite o dettagli non rilevanti, nel rispetto dei principi di pertinenza e non eccedenza. La localizzazione delle telecamere e le modalità di ripresa saranno quindi stabilite in modo conseguente.

Valutazione : Accettabile

I dati sono esatti e aggiornati?

I dati vengono aggiornati periodicamente, almeno su base annuale, e incrociati con le banche dati nazionali.

Valutazione : Accettabile

Qual è il periodo di conservazione dei dati?

I dati personali registrati mediante l'utilizzo degli impianti di videosorveglianza di cui al presente Regolamento sono conservati per un periodo di tempo non superiore a sette giorni dalla data della rilevazione. Decorso tale periodo, i dati registrati sono cancellati con modalità automatica. Gli strumenti e i supporti elettronici utilizzati sono dotati dei sistemi di protezioni che garantiscono la tutela dei dati trattati.

Valutazione : Accettabile

Misure a tutela dei diritti degli interessati
Come sono informati del trattamento gli interessati?

Gli interessati sono informati nei seguenti modi:
a) pubblicazione sul sito internet istituzionale di planimetrie e di altra documentazione relative alle zone videosorvegliate e foto-sorvegliate;
b) installazione di apposita segnaletica permanente contenente l'informativa minima nelle aree in cui sono concretamente posizionate le telecamere, di cui al già richiamato Provvedimento in materia di videosorveglianza del Garante per la Protezione dei dati Personali del 08/04/2010. Sono fatti salvi i casi di prevenzione, accertamento o repressione dei reati.
c) informativa contenente gli elementi di cui all'art. 13 e 14 del Regolamento UE 2016/679 disponibile agevolmente senza oneri per gli interessati con modalità facilmente accessibili anche con strumenti informatici o telematici.
d) La segnaletica deve essere collocata prima del raggio di azione della telecamera, o nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti; la stessa deve avere un formato ed un posizionamento tale da essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno.
e) In presenza di più telecamere, in relazione alla vastità dell'area e alle modalità delle riprese, andranno installati più cartelli informativi.
f) L'Ente, nella persona del Titolare del trattamento dei dati, si obbliga ad informare la comunità cittadina dell'avvio del trattamento dei dati personali, con l'attivazione dell'impianto di videosorveglianza, dell'eventuale incremento dimensionale dell'impianto stesso e dell'eventuale successiva cessazione per qualsiasi causa del trattamento medesimo

Valutazione : Accettabile

Ove applicabile: come si ottiene il consenso degli interessati?

Essendo l'ente una pubblica amministrazione che eroga servizi pubblici legalmente attribuiti non è tenuto all'acquisizione del consenso al trattamento dei dati, nei casi in cui questo sia dovuto viene acquisito per iscritto.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?

1. In relazione al trattamento di dati personali che lo riguardano, l'interessato, in ossequio alle disposizioni di cui agli artt. 15 e ss., RGPD, su presentazione di apposita istanza, ha diritto:
a) di ottenere dal titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e, in tal caso, di ottenere l'accesso ai dati stessi;
b) ad essere informato sulle finalità e le modalità del trattamento dei dati, sugli eventuali destinatari o categorie di destinatari a cui i dati personali potranno essere comunicati, sul periodo di conservazione dei dati personali;
c) di richiedere la cancellazione qualora sussista uno dei motivi di cui all'art. 17 RGPD, la trasformazione in forma anonima o il blocco dei dati trattati in violazione di legge, compresi quelli di cui non è necessaria la conservazione in relazione agli scopi per i quali i dati sono stati raccolti o successivamente trattati;
d) di opporsi, in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano, ai sensi dell'art. 21, RGPD.
2. L'istanza per l'esercizio dei diritti dell'interessato è presentata al Responsabile della Protezione dei dati dell'Ente, ai sensi dell'art. 38, paragrafo 4, RGDP ovvero al Responsabile del trattamento dei dati individuato.
3. Nel caso di richiesta di accesso alle immagini, l'interessato dovrà provvedere ad indicare:
a) il luogo, la data e la fascia oraria della possibile ripresa;
b) l'abbigliamento indossato al momento della possibile ripresa;
c) gli eventuali accessori in uso al momento della possibile ripresa;
d) l'eventuale presenza di accompagnatori al momento della possibile ripresa;
e) l'eventuale attività svolta al momento della possibile ripresa;
f) eventuali ulteriori elementi utili all'identificazione dell'interessato.
4. Il responsabile della protezione dei dati dell'Ente ovvero il responsabile del trattamento accerterà l'effettiva esistenza delle immagini e di ciò darà comunicazione al richiedente; nel caso di accertamento positivo fisserà altresì il giorno, l'ora ed il luogo in cui l'interessato potrà prendere visione delle immagini che lo riguardano.
5. Qualora, ai sensi dell'art. 15, paragrafo 3, RGPD, l'interessato chieda di ottenere una copia dei dati personali oggetto di trattamento, si procederà al rilascio dei files contenenti le immagini in un formato elettronico di uso comune, previo oscuramento dei dati identificativi riferiti alle altre persone fisiche eventualmente presenti al momento della ripresa, in ossequio alla previsione di cui all'art. 15, paragrafo 4, RGPD.
6. I diritti di cui al presente articolo riferiti ai dati personali concernenti persone decedute possono essere esercitati da chi ha un interesse proprio, o agisce a tutela dell'interessato o per ragioni familiari meritevoli di protezione.
7. Nell'esercizio dei diritti di cui al comma 1 l'interessato può conferire, per iscritto delega o procura a persone fisiche, enti, associazioni od organismi. L'interessato può altresì farsi assistere da persona di fiducia.

Le istanze di cui al presente articolo possono essere trasmesse al titolare o al responsabile anche mediante lettera raccomandata o posta elettronica certificata, nel caso di esito negativo alla istanza l'interessato può rivolgersi al Garante per la protezione dei dati personali, fatte salve le possibilità di tutela amministrativa e giurisdizionale previste dalla normativa vigente.

Possono essere adottate misure legislative intese a ritardare, limitare o escludere la comunicazione di informazioni all'interessato e per il tempo in cui ciò costituisca una misura necessaria e proporzionata in una società democratica, tenuto debito conto dei diritti fondamentali e dei legittimi interessi della persona fisica interessata al fine di:

1 . Non compromettere indagini, inchieste o procedimenti ufficiali o giudiziari;

.2. Non compromettere la prevenzione, l'indagine, l'accertamento e il perseguimento di reati o l'esecuzione di sanzioni penali; .3. Proteggere la sicurezza pubblica; .4. Proteggere la sicurezza nazionale;

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?

Per esercitare il diritto alla cancellazione, se possibile in ragione dell'obbligo dell'ente di conservazione delle informazioni, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?

Per esercitare il diritto di limitazione o opposizione, se possibile, gli interessati possono contattare direttamente il titolare o il designato del trattamento dei dati recandosi direttamente presso l'ente, a mezzo raccomandata o posta elettronica certificata.

Valutazione : Accettabile

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

Gli obblighi di ogni singolo responsabile del trattamento sono definiti nei contratti di appalto dei relativi servizi o con specifica comunicazione.

Valutazione : Accettabile

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
I dati non vengono trasferiti al di fuori dell'Unione Europea.

Valutazione : Accettabile

Rischi

Misure esistenti o pianificate

Anonimizzazione

I particolari tipi di dati, ovvero i C.d. dati sensibili, vengono trattati in maniera riservata unicamente dal personale strettamente necessario e a questo autorizzato, vengono resi sempre completamente anonimi quando pubblicati.

Valutazione : Accettabile

Controllo degli accessi logici

Ogni operatore una postazione fisica assegnata con cassetti muniti di chiavi se previsti e una postazione informatica dedicata dotata di username e password univoca di accesso.

Valutazione : Accettabile

Tracciabilità

Il software prevede la registrazione e conseguente tracciabilità degli accessi logici e delle operazioni effettuate dagli autorizzati al trattamento dati.

Valutazione : Accettabile

Archiviazione

Ogni responsabile controlla l'archiviazione dei dati gestiti dall'ufficio in una cartella non condivisa su una postazione informatica protetta da password, mentre gli archivi generali dell'ente sono conservati su un server dedicato il cui accesso è limitato e controllato. Per quanto riguarda l'archiviazione cartacea questa avviene all'interno degli uffici che trattano i dati e viene garantito l'anonimato delle informazioni contenute, per quanto riguarda i particolari tipi di dati vengono previste delle misure di protezione ulteriori e specifiche come armadietti con chiusura a chiave o casseforti.

Valutazione : Accettabile

Sicurezza dei documenti cartacei

I documenti cartacei vengono conservati dai dipendenti dell'ufficio, il responsabile verifica che siano disposti in specifici raccoglitori in moda tale che non vadano dispersi e che non siano visibili a terzi non autorizzati, gli uffici devono essere chiusi e l'accesso consentito soltanto agli addetti o ai soggetti autorizzati.

Valutazione : Accettabile

Minimizzazione dei dati
Vengono raccolti e conservati unicamente i dati necessari all'erogazione del servizio.

Valutazione : Accettabile

Vulnerabilità

I software in uso vengono aggiornati costantemente e l'accesso ai dati è limitato unicamente agli operatori direttamente interessati ai quali viene assegnato un account univoco e tracciabile.

Valutazione : Accettabile

Lotta contro il malware

L'antimalware è regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Backup
Backup giornaliero

Valutazione : Accettabile

Sicurezza dei canali informatici

Il firewall risulta regolarmente istallato e costantemente aggiornato.

Valutazione : Accettabile

Manutenzione

La manutenzione fisica dei dispositivi viene effettuata all'occorrenza.

Valutazione : Accettabile

Controllo degli accessi fisici

Gli accessi fisici agli uffici sono limitati e controllati.

Valutazione : Accettabile

Prevenzione delle fonti di rischio

Gli uffici dell'ente risultano rispettare le previsioni normative in materia di salute e protezione sui luoghi di lavoro.

Valutazione : Accettabile

Gestione delle politiche di tutela della privacy

Le politiche di tutela alla privacy comprendono il regolamento sulla videosorveglianza adottato dall'ente, nonchè l'osservanza del Regolamento UE 679/2016 con relativa nomina DPO

Valutazione : Accettabile

Gestione del personale
I dipendenti sono regolarmente invitati a partecipare ad incontri di formazione al fine di essere istruiti sul corretto trattamento dei dati personali.

Valutazione : Accettabile

Specifiche misure di sicurezza
Ai sensi di quanto previsto dall'articolo 24 del Reg. UE 201 6/679, i dati personali acquisiti mediante l'utilizzo degli impianti di videosorveglianza e sono protetti da misure di sicurezza tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato e trattamento non consentito o non conforme alle finalità di cui all'articolo 3 del presente Regolamento.

Ai sensi dell'art. 29 c. 2 della Direttiva UE 201 6/680 il Titolare del trattamento, previa valutazione dei rischi, mette in atto misure volte a:

a. Vietare alle persone non autorizzate l'accesso alle attrezzature utilizzate per il trattamento («controllo dell'accesso alle attrezzature»);

b. Impedire che supporti di dati possano essere letti, copiati, modificati o asportati da persone non autorizzate («controllo dei supporti di dati»);

c. Impedire che i dati personali siano inseriti senza autorizzazione e che i dati personali conservati siano visionati, modificati o cancellati senza autorizzazione («controllo della conservazione»);

d. Impedire che persone non autorizzate utilizzino sistemi di trattamento automatizzato mediante attrezzature per la trasmissione di dati («controllo dell'utente)
e. Garantire che le persone autorizzate a usare un sistema di trattamento automatizzato abbiano accesso solo ai dati personali cui si riferisce la loro autorizzazione d'accesso («controllo dell'accesso ai dati»);

f. Garantire la possibilità di verificare e accertare gli organismi ai quali siano stati o possano essere trasmessi o resi disponibili i dati personali utilizzando attrezzature per la trasmissione di dati («controllo della trasmissione»);

g. Garantire la possibilità di verificare e accertare a posteriori quali dati personali sono stati introdotti nei sistemi di trattamento automatizzato, il momento della loro introduzione e la persona che l'ha effettuata («controllo dell'introduzione»);

h. Impedire che i dati personali possano essere letti, copiati, modificati o cancellati in modo non autorizzato durante i trasferimenti di dati personali o il trasporto di supporti di dati («controllo del trasporto»);

i. Garantire che, in caso di interruzione, i sistemi utilizzati possano essere ripristinati («recupero»);

j. Garantire che le funzioni del sistema siano operative, che eventuali errori di funzionamento siano segnalati («affidabilità») e che i dati personali conservati non possano essere falsati da un errore di funzionamento del sistema («integrità»).

Valutazione : Accettabile

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Impatto limitato

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Perdita di dati, uso improprio di dati, diffusione di dati riservati o sensibili.

Quali sono le fonti di rischio?
Fonti di rischio interne ed esterne anche non umane.

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Controllo degli accessi logici, Tracciabilità, Minimizzazione dei dati, Anonimizzazione, Sicurezza dei documenti cartacei, Gestione delle politiche di tutela della privacy, Prevenzione delle fonti di rischio

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Il rischio è limitato, vengono riprese soprattutto i numeri di targa degli autoveicoli e le immagini sono conservate solo in caso di necessità di tutela della publica sicurezza.

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, Secondo le misure pianificate il rischio è trascurabile.

Valutazione : Accettabile

Modifiche indesiderate dei dati
Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Impatto limitato

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Errore materiale, evento doloso o abuso di ufficio da parte degli addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzati.

Quali sono le fonti di rischio?
Fonti umane interne, fonti umane esterne, fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Backup, Sicurezza dei canali informatici, Manutenzione, Vulnerabilità, Controllo degli accessi fisici, Prevenzione delle fonti di rischio, Lotta contro il malware, Controllo degli accessi logici, Specifiche misure di sicurezza

Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Limitata

Perdita di dati
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Impatto limitato

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Errore materiale, evento doloso o abuso di ufficio da parte di addetti ai lavori, accesso ai dati da parte di soggetti esterni non competenti e non autorizzate., Attacco hacker

Quali sono le fonti di rischio?

Fonti umane interne, fonti umane esterne, fonti non umane.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?

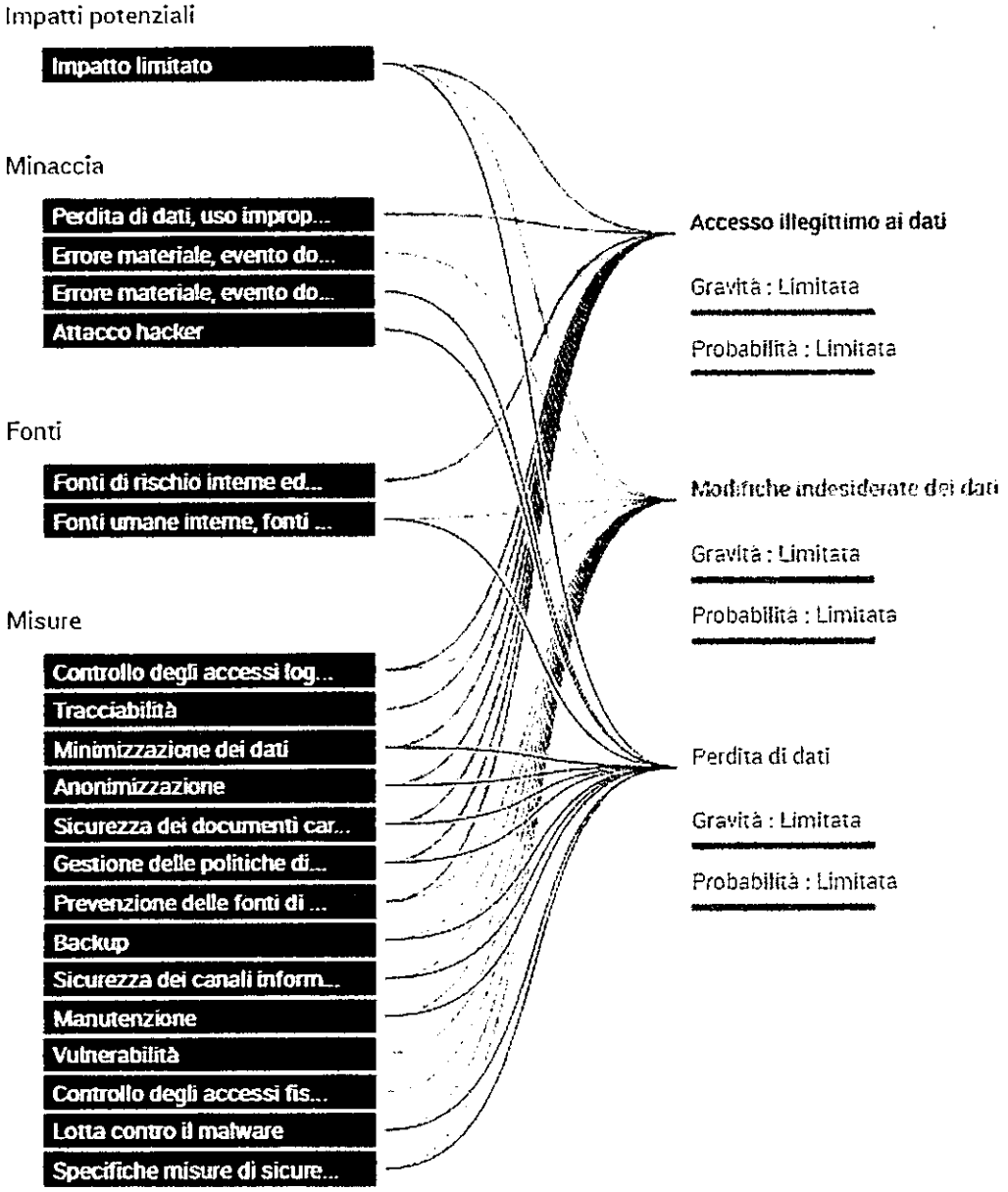
Minimizzazione dei dati, Sicurezza dei canali informatici, Lotta contro il malware, Backup, Manutenzione, Gestione delle politiche di tutela della privacy, Anonimizzazione, Sicurezza dei documenti cartacei, Specifiche misure di sicurezza

Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

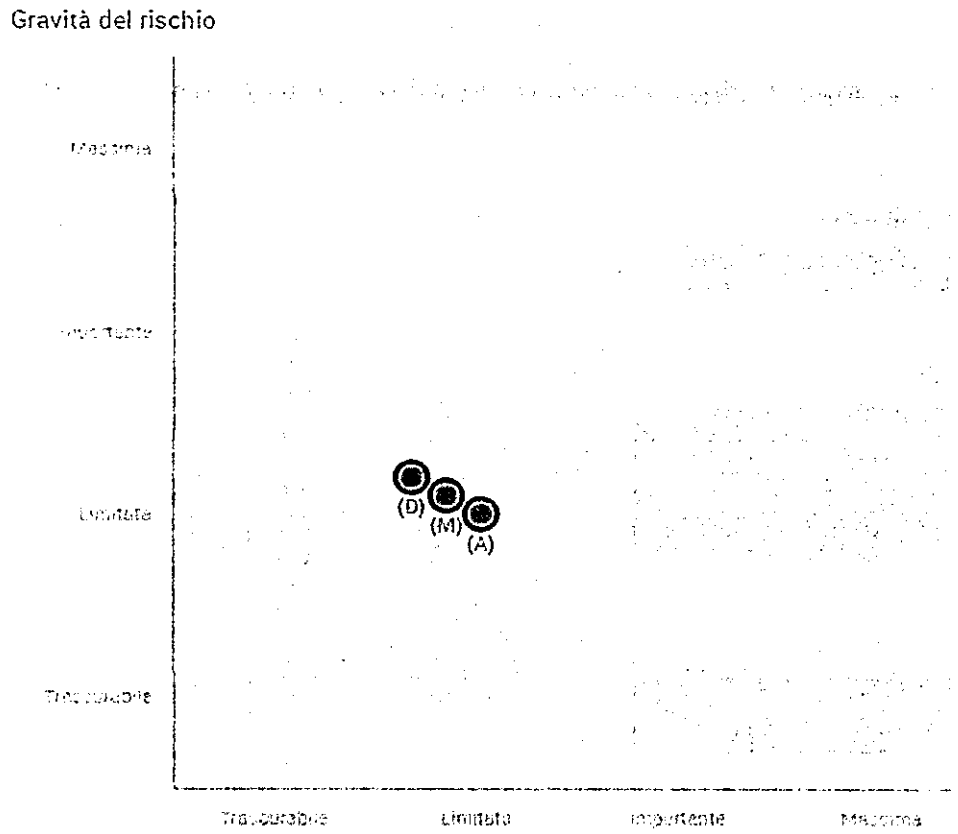
Limitata

Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?

Limitata



MAPPATURA DEL RISCHIO



- Misure pianificate o esistenti
- Con le misure correttive implementate
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Letto, approvato e sottoscritto

IL SINDACO

L'ASSESSORE ANZIANO

IL SEGRETARIO GENERALE

CERTIFICATO DI PUBBLICAZIONE

La presente deliberazione viene pubblicata per 15 giorni consecutivi all'Albo Pretorio online del Comune, sul sito istituzionale dell'Ente: **www.comune.modica.gov.it.**

Modica lì

Il Segretario Generale

Si attesta che copia della presente deliberazione è stata pubblicata all'Albo Pretorio online del Comune di Modica, senza opposizioni e reclami, dal 12 APR 2021 al 27 APR 2021, ed è repertoriata nel registro delle pubblicazioni al n. _____.

Modica lì

Il Responsabile della pubblicazione

ATTESTAZIONE DI ESECUTIVITA'

La presente deliberazione:

☒ E' stata dichiarata immediatamente esecutiva ai sensi dell'art.12, comma 2, della L.R. 44/91.

☐ E' divenuta esecutiva il _____ ai sensi dell'art. 12, comma 1, della L.R. 44/91, trascorsi dieci giorni dall'inizio della pubblicazione.

Modica lì

Il Segretario Generale

Per copia conforme all'originale ad uso amministrativo.

Modica lì

Il Segretario Generale