



Comune di Maddaloni

* * *

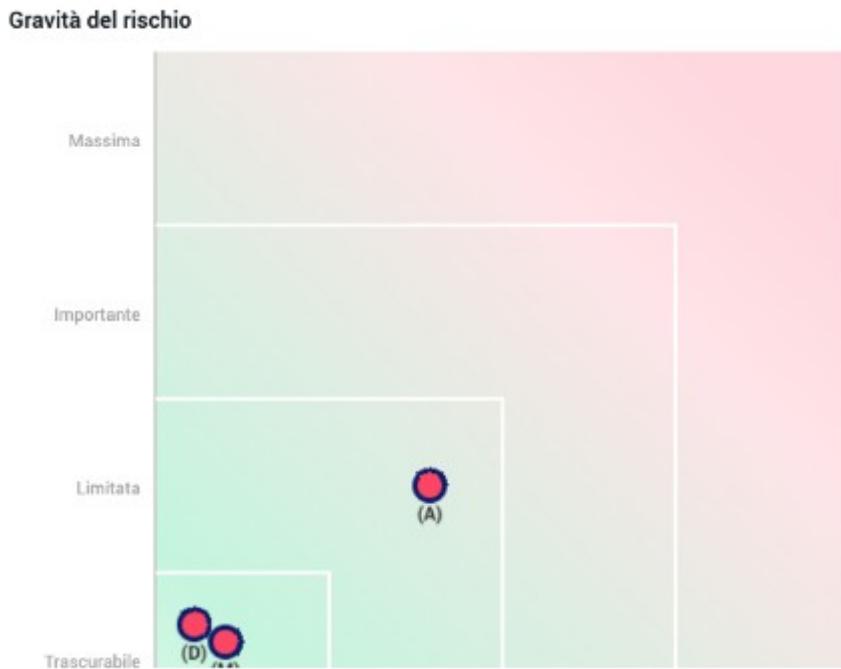
DATA PROTECION IMPACT ASSESSMENT (DPIA)

Data Privacy Officer
Dott. Vincenzo de Prisco

Il Sindaco
Andrea De Filippo

Editing	Dott. Vincenzo de Prisco – Data Privacy Officer
Evaluation	Dott. Vincenzo de Prisco – Data Privacy Officer
Validation	Dott. Vincenzo de Prisco – Data Privacy Officer
Status	Validata 100%

Mappaggio dei rischi



Piano d'azione

Panoramica

Principi fondamentali	Misure esistenti o pianificate
Finalità	Crittografia
Basi legali	Anonimizzazione
Adeguatezza dei dati	Tracciabilità
Esattezza dei dati	
Periodo di conservazione	
Informativa	
Raccolta del consenso	

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

DPO and data subjects opinion

Nome del DPO/RPD

Vincenzo De Prisco

Posizione del DPO/RPD

Il trattamento può essere implementato.

Parere del DPO/RPD

Conoscenza della struttura, verrà gestita tuttavia una ulteriore procedura per gli acquisti informatici aderente alla determina 220/2020 AGID

Richiesta del parere degli interessati

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati

Non necessaria, faziosa

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Il trattamento ha ad oggetto i dati personali (immagini) raccolti mediante l'attivazione e il funzionamento di un impianto di videosorveglianza attivo presso la sede del Comune di Maddaloni -CE-. L'impianto di videosorveglianza è installato per il perseguitamento delle seguenti finalità

- tutela del patrimonio dell'ente
- sicurezza urbana
- deterrenza
- gestione del territorio
- esigenze organizzative e produttive

L'impianto è costituito da 50 telecamere, due DVR ed è garantita la resilienza e la scalabilità del sistema dall'ufficio CED.

Delle telecamere computate 11 sono in grado di leggere il numero di targa dell'automezzo ripreso, 30 sono sensibili ad eventi e capaci di far iniziare un ciclo logico programmabile, 12 sono di tipo deep learning. Queste ultime sono quelle per le quali la discrezionalità della redazione dell'impatto ex art 35 Reg. 2016/679 viene ridotta. Sempre per queste ultime si rimanda l'attenzione ai sistemi AI che verranno disciplinati dall'AI ACT.

Criticità del trattamento: risiede nel fatto che dal funzionamento dell'impianto di videosorveglianza potrebbe derivare un controllo a distanza delle attività dei lavoratori, riconducibile all'articolo 35, paragrafo 3, lettera c), GDPR, nella fattispecie di "Monitoraggio sistematico, trattamenti utilizzati per osservare monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o sorveglianza sistematica di un'area accessibile al pubblico".

Quali sono le responsabilità connesse al trattamento?

Titolare del Trattamento: Comune di Maddaloni , dati salienti di contatto <https://indicepa.gov.it/ippa-portale/consultazione/indirizzo-sede/ricerca-ente/scheda-ente/7153>

- *Responsabile del Trattamento: il responsabile deve avere almeno i requisiti dell'art 28 GDPR*
- *Data Protection Officer: Il Titolare si avvale di un Responsabile per la protezione dei dati personali (anche noto come Data Protection Officer "DPO") che vigila sulla conformità aziendale alla normativa a protezione dei dati personali. Il DPO può essere contattato tramite il seguente canale di comunicazione: Vincenzo De Prisco, cell. 3389141276, mail segreteria@ca-campania.com*
- *Incaricati del trattamento: Si rimanda al regolamento di Videosorveglianza*

Ci sono standard applicabili al trattamento?

Al trattamento in materia di videosorveglianza si applicano le seguenti normative e provvedimenti:

- Art. 4 L. 300/1970 (c.d. Statuto dei Lavoratori), così come modificato dall'art. 23 del D.lgs. 151/2015 (c.d. Jobs Act);
- Regolamento UE n. 2016/679 (GDPR);

- D.Lgs. n. 196/2003 (c.d. Codice Privacy) così come novellato dal D.Lgs. 101/2018;
- EDPB, Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video (adottate il 29 gennaio 2020);
- Provvedimento generale in materia di videosorveglianza dell'8 aprile 2010.

Valutazione : Accettabile

Commento di valutazione : gestito

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Le immagini di videosorveglianza consentono l'identificazione della persona fisica (dipendente/visitatore/collaboratore esterno/fornitore) che può essere identificata, direttamente o indirettamente, in particolare con riferimento a un identificativo come il nome, un numero di identificazione, oltre che più elementi caratteristici della sua identità fisica e fisiologica. Altresì permettono l'individuazione di soggetti fisici dall'interrogazione di altri dati certi, ad esempio dal numero di targa,

Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?

Il Titolare del trattamento Comune di Maddaloni raccoglie i dati personali mediante il funzionamento dell'impianto di videosorveglianza attivo sul territorio dell'Ente. Le immagini, oltre che essere viste in tempo reale vengono registrate mediante il Sistema CCTV-DVR, il quale trasmette le immagini acquisite su monitor dedicati e controllati dal personale incaricato della videosorveglianza. L'accesso alle immagini registrate avviene solo nel caso si verifichino eventi criminosi o eventi che rendano necessario un intervento. I dati personali non vengono diffusi e/o divulgati, ma vengono comunicati esclusivamente all'Autorità giudiziaria e/o di polizia per rispondere a particolari esigenze d'indagine. Alla fine del periodo di 7 giorni le immagini vengono cancellate mediante sovrascrittura automatica. E' onere del DPO nominato fare controlli a campione per il rispetto della sovrascrittura.

Quali sono le risorse di supporto ai dati?

Il Sistema CCTV comporta la raccolta e il trattamento dei dati personali raccolti tramite videosorveglianza, quindi su supporto elettronico. I supporti sono di seguito elencati con ulteriori indicazioni della tipologia, in particolare i supporti DEEP LEARNING sono riportati in **GRASSETTO**

La validità della DPIA , considerata la standardizzazione di modelli di telecamera che rimangono fissi anche in eventuali estensioni future , può considerarsi adeguata.

Tipologia	Quantità
AXIS P1343	4
AXIS Q6032	1
DS-2CD2655FWD-IZS	2

DS-2CD2685FWD-IZS	9
DS-2CD3686G2-IZS	9
DS-2CD4A26FWD-IZS/P	2
DS-2DE4425IW-DE	8
DS-2DF6A425X-AEL	3
ids TCM 203-A	12
Totale Risultato	50

Valutazione : Accettabile

Commento di valutazione :

La valutazione è favorevole vista la presenza di procedure :

- tecnologiche
- organizzative
- giuridiche

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, esplicativi e legittimi?

Gli scopi sono specifici, esplicativi e legittimi, in quanto i dati personali sono raccolti e trattati dal comune di Maddaloni esclusivamente per finalità di sicurezza (pubblica), controllo degli accessi (veicolari), tutela istituzionale, incolumità fisica delle persone ai sensi della normativa sulla sicurezza nei luoghi di lavoro, tutela di proprietà e patrimonio dell'Ente.

Valutazione : Accettabile

Commento di valutazione :

Il trattamento è finalizzato alla gestione di una base giuridica disciplinata dal Reg. 2016/679.

Quali sono le basi legali che rendono lecito il trattamento?

Base giuridica: il trattamento si fonda sulla base giuridica del legittimo interesse del Titolare del trattamento (articolo 6, paragrafo 1, lettere c) e) f) GDPR).

Valutazione : Accettabile

Commento di valutazione :

Conformato articolo 6 ed articolo 9 Reg. 2016/679

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 del principio della pertinenza delle immagini raccolte, il Sistema CCTV non è installato, ad esempio, in quei luoghi dove i rischi connessi alle finalità di cui sopra sono del tutto assenti e, al contrario, è incentivata l'adozione di strumenti tecnologici conformati già in origine in modo da non utilizzare dati relativi a persone identificabili quando le finalità del trattamento possono essere realizzate

impiegando solo dati anonimi. In particolare, le telecamere sono installate affinché l'angolatura e la panoramica delle riprese venga effettuata con modalità tali da limitare l'angolo di visuale all'area da proteggere .

Valutazione : Accettabile

Commento di valutazione :

Dati essenziali

I dati sono esatti e aggiornati?

I dati sono raccolti in tempo reale e archiviati decorso il termine di conservazione previsto, quindi sono costantemente esatti e aggiornati.

Valutazione : Accettabile

Commento di valutazione :

Dati sempre aggiornati. Per le notificazioni i dati sono aggiornati con anche gli istituti propri delle comunicazioni del D.lgs 82705 (6 bis e 6 quater)

Qual è il periodo di conservazione dei dati?

La conservazione delle immagini registrate dal Sistema CCTV è limitata al tempo, segnatamente 7 giorni. Il Sistema CCTV è programmato in modo da prevedere l'integrale cancellazione automatica delle informazioni allo scadere del termine previsto, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati.

Valutazione : Accettabile

Commento di valutazione :

Previsto norme, prassi, regolamenti, provvedimenti AAI

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Gli interessati al trattamento sono informati tramite le seguenti modalità:

- informativa semplificata (cartelli) che vengono apposti in prossimità delle aree video-sorvegliate;
- informativa estesa redatta ai sensi dell'articolo 13 GDPR, che viene fatta sottoscrivere ai dipendenti per presa visione.

Valutazione : Accettabile

Commento di valutazione :

Conforme

Ove applicabile: come si ottiene il consenso degli interessati?

Per il trattamento in oggetto non è richiesto il consenso dell'interessato, in quanto si fonda su un presupposto di liceità diverso (legittimo interesse del Titolare - articolo 6, paragrafo 1, lettere c) e) f),

GDPR).

Valutazione : Accettabile

Commento di valutazione :

Conforme

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

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo al Titolare od al DPO al seguente indirizzo : segreteria@ca-campania.com, lo stesso è raggiungibile anche al recapito mobile 3389141276, il nominativo comunicato è VINCENZO DE PRISCO

Valutazione : Accettabile

Commento di valutazione :

verificato

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

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo al Titolare od al DPO al seguente indirizzo : segreteria@ca-campania.com, lo stesso è raggiungibile anche al recapito mobile 3389141276, il nominativo comunicato è VINCENZO DE PRISCO

Valutazione : Accettabile

Commento di valutazione :

canali collaudati

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

L'interessato può in qualsiasi momento esercitare i diritti di cui agli artt. 15-22 GDPR, scrivendo al Titolare od al DPO al seguente indirizzo : segreteria@ca-campania.com, lo stesso è raggiungibile anche al recapito mobile 3389141276, il nominativo comunicato è VINCENZO DE PRISCO

Valutazione : Accettabile

Commento di valutazione :

canali collaudati

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

L'elenco dei RESPONSABILI ex articolo 28 è costantemente aggiornato, vista la dinamicità del calcolo dell'impatto si rimanda ai documenti amministrativi.

Valutazione : Accettabile

Commento di valutazione :

revisioni dei contratti

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?

I dati trattati restano in SSE.

Valutazione : Accettabile

Commento di valutazione :

Nessun dato fuori SSE ,

Rischi

Misure esistenti o pianificate

Crittografia

I dati registrati sui sistemi sono crittografati.

Valutazione : Accettabile

Commento di valutazione :

Il sistema di crittografia è ad oggi valido e la scelta del produttore garantisce gli aggiornamenti tecnologici.

L'ufficio CED monitora gli allarmi ACN e CSIRT.

IL DPO monitora gli allarmi ACN e CSIRT.

Anonimizzazione

I dati sono resi anonimi e non collegati ad eventi

Valutazione : Accettabile

Commento di valutazione :

L'ufficio CED monitora gli allarmi ACN e CSIRT.

IL DPO monitora gli allarmi ACN e CSIRT.

Tracciabilità

Il sistema dei LOG garantisce una catena sicura.

Valutazione : Accettabile

Commento di valutazione :

Controlli del DPO e del RTD.

Accesso illegittimo ai dati

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

Perdita di fiducia, Perdita di confidenzialità

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Intrusione nei sistemi del titolare, intrusione nei sistemi del responsabile

Quali sono le fonti di rischio?

UMANE INTERNE, UMANE ESTERNE, NON UMANE, INTELLIGENZA ARTIFICIALE
MALEVOLI

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Crittografia, Anonimizzazione, Tracciabilità

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

Limitata, L'IMPATTO sarà appena superiore a quello TRASCURABILE, viste le procedure ed i dati trattati.

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

Limitata, viste le procedure ed i continui aggiornamenti, gli attori coinvolti (titolare, responsabile, DPO del titolare e DPO del responsabile) i rischi sono limitati.

Valutazione : Accettabile

Commento di valutazione :

Impatto e probabilità mitigati

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Perdita di confidenzialità, Perdita di fiducia

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?

Intrusione nei sistemi del responsabile, Intrusione nei sistemi del titolare

Quali sono le fonti di rischio?

INTELLIGENZA ARTIFICIALE MALEVOLA, NON UMANE, UMANE ESTERNE, UMANE INTERNE

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

Crittografia, Anonimizzazione, Tracciabilità

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

Trascurabile, Gravità altresì ridotta dalla resilienza e dalla manifestazione prevalentemente interna

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

Trascurabile, Ad oggi con i presidi adottati ed il continuo aggiornamento dei driver coinvolti il rischio p trascurabile

Valutazione : Accettabile

Commento di valutazione :

Impatto e probabilità gestito

Perdita di dati

Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?

Perdita di fiducia, Perdita di confidenzialità

Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?

Intrusione nei sistemi del titolare, intrusione nei sistemi del responsabile

Quali sono le fonti di rischio?

INTELLIGENZA ARTIFICIALE MALEVOLA, NON UMANE, UMANE ESTERNE, UMANE INTERNE

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

Crittografia, Anonimizzazione, Tracciabilità

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

Trascurabile, Nessuna importanza per i dati già crittografati

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

Trascutabile, viste le procedure ed i continui aggiornamenti, gli attori coinvolti (titolare, responsabile, DPO del titolare e DPO del responsabile) i rischi sono limitati.

Valutazione : Accettabile

Commento di valutazione :

gestito con diverse procedure di diversi soggetti

Panoramica dei rischi

Impatti potenziali

Perdita di fiducia
Perdita di confidenzialità

Minaccia

Intrusione nei sistemi del ..
intrusione nei sistemi del ..

Accesso illegittimo ai dati

Gravità : Limitata

Probabilità : Limitata

Fonti

UMANE INTERNE
UMANE ESTERNE
NON UMANE
INTELLIGENZA ARTIFICIALE

Modifiche indesiderate dei dati

Gravità : Trascutabile

Probabilità : Trascutabile

Misure

Crittografia
Anonimizzazione
Tracciabilità

Perdita di dati

Gravità : Trascutabile

Probabilità : Trascutabile