

Informazioni sulla PIA

Nome della PIA

Dati da telecamere e riprese

Nome autore

Scandicci

Nome valutatore

Scandicci

Nome validatore

Gruppo lavoro 6 comuni

Data di creazione

05/03/2019

Allegati

20190304-SalaServer-Studiofattibilità.pdf

20190305-PDO2019-SettoreII-Chiarelli-Settore.pdf

20190305-PDO2019-SettoreII-Chiarelli-UO-2-1.pdf

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?

Trattamento dati da riprese video, audio e fotogrammi nell'ambito di varie attività dell'Ente fra cui:

- videosorveglianza con funzioni di sicurezza, controllo del patrimonio pubblico, protezione civile, sedute del consiglio comunale o altri eventi pubblici
- infrazioni in materia ambientale
- infrazioni al codice della strada
- controllo della circolazione veicolare

Quali sono le responsabilità connesse al trattamento?

Titolare dei trattamenti è il Comune che opera tramite i propri uffici e servizi deputati alle varie attività, in collaborazione con soggetti esterni istituzionali (autorità di sicurezza) e professionali (responsabili).

Responsabili: come da pubblicazione nella sezione privacy del sito web istituzionale dell'Ente.

Ci sono standard applicabili al trattamento?

I principali standard sono collegati alle caratteristiche tecniche e tecnologiche dei prodotti. Dal punto di vista di processo e degli adempimenti si fa riferimento a:

- Provvedimento del Garante Privacy 8 aprile 2010 doc n. 1712680
- Codice della strada e regolamento attuativo e disposizioni di attuazione
- Regolamento comunale in materia di videosorveglianza
- Disposizioni comunali sul trattamento dei dati

Valutazione : Accettabile

Commento di valutazione :

Versione rivista dopo incontro del 5 marzo 2019

Dati, processi e risorse di supporto

Quali sono i dati trattati?

I principali dati trattati sono:

- immagini (fotogrammi)
- immagini (video)
- dati elaborati da targhe di veicoli

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

L'ordinario ciclo di vita del trattamento è dato da:

- raccolta dei dati (automatizzata)
- registrazione e conservazione (automatizzata)
- elaborazione (automatizzata e tramite personale autorizzato)
- (eventuali) trattamenti conseguenti all'elaborazione
- (eventuale) archiviazione per i tempi del procedimento
- distruzione, cancellazione (automatizzata e tramite personale autorizzato)

Quali sono le risorse di supporto ai dati?

Le principali risorse sono:

- Hardware e software dedicato
- Personale autorizzato al trattamento dei dati (dell'Ente o dei Responsabili del trattamento)
- locali e/o archivi contenenti documentazione analogica

Valutazione : Accettabile

Commento di valutazione :

Da integrare dopo l'incontro del gruppo di lavoro del 5 marzo 2019

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Scopi del trattamento:

- funzioni di sicurezza, controllo del patrimonio pubblico, protezione civile, sedute del consiglio comunale o altri eventi pubblici tramite video riprese
- infrazioni in materia ambientale, tramite video trappole
- infrazioni al codice della strada, tramite rosso semaforico, autovelox, tele laser, targa system, ...
- controllo della circolazione veicolare, tramite porte telematiche, ...

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Quali sono le basi legali che rendono lecito il trattamento?

art. 6 c. 1 lett. c), d), e) e f) Regolamento UE 2016/679

D.Lgs. 196/2003 e s.m.i.

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Rispetto del principio di minimizzazione

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

I dati sono esatti e aggiornati?

Rispetto del principio

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Qual è il periodo di conservazione dei dati?

- funzioni di sicurezza, controllo del patrimonio pubblico, protezione civile, sedute del consiglio comunale o altri eventi pubblici tramite video riprese: termine minimo previsto dalle norme di settore, e comunque non superiore a sette giorni
- per i trattamenti derivanti da elaborazione dei dati, valgono i termini previsti nel Manuale di gestione del protocollo informatico e dei flussi documentali

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?

Informativa specifica:

- fornita a sportello
 - fornita nei form di raccolta dati dei servizi online
 - nella sezione privacy del sito web istituzionale dell'Ente
- Idonea cartellonistica presso i punti di raccolta dei dati

Valutazione : Da correggere

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Ove applicabile: come si ottiene il consenso degli interessati?

I trattamenti sono generalmente effettuati in base a obbligo legale o per la tutela di interessi dell'interessato o dell'ente e solo episodicamente sulla base di consenso espresso (per trattamenti ulteriori o finalità specifiche). In questi casi il consenso è acquisito previa informativa specifica.

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Utilizzo di specifica modustica pubblicata nella sezione privacy del sito web istituzionale dell'Ente o resa disponibile presso gli sportelli (a richiesta)

Valutazione : Da correggere

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Utilizzo di specifica modustica pubblicata nella sezione privacy del sito web istituzionale dell'Ente o resa disponibile presso gli sportelli (a richiesta)

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Utilizzo di specifica modustica pubblicata nella sezione privacy del sito web istituzionale dell'Ente o resa disponibile presso gli sportelli (a richiesta)

Valutazione : Da correggere

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Sì. I contratti di servizi per la gestione dei dati contengono clausole espresse o di rinvio sulle modalità di trattamento dati nel rispetto di quanto previsto dal regolamento UE 2016/679

Valutazione : Da correggere

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

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

Pur non essendo generalmente previsti trasferimenti dati al di fuori della U.E. in tali episodici casi saranno adottate modalità di protezione equivalenti (es. in caso di ricerche presso autorità straniere di targhe o dati personali).

Valutazione : Da correggere

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Misure esistenti o pianificate

Controllo degli accessi logici

Abilitazioni all'accesso secondo le normali procedure di rilascio credenziali

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Tracciabilità

Secondo criteri ordinari di tracciabilità, tempi di conservazione allineati a quelli del trattamento

Valutazione : Accettabile

Archiviazione

Politiche di backup dei dati elettronici

Valutazione : Accettabile

Sicurezza dei documenti cartacei

Vedasi Manuale di Gestione dle protocollo informatico e dei flussi documentali

Valutazione : Accettabile

Minimizzazione dei dati

- non sono effettuate elaborazioni automatiche dei dati
- si elaborano i soli dati rilevanti ai fini dell'avvio di un procedimento amministrativo sanzionatorio

Valutazione : Accettabile

Vulnerabilità

Ordinarie politiche di prevenzione

Valutazione : Accettabile

Gestione postazioni

Accesso ai client di dominio con credenziali personali, ordinarie politiche di sicurezza delle credenziali

Valutazione : Accettabile

Backup

Backup e conservazione secondo ordinari standard tecnologici e di sicurezza

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Manutenzione

Tramite contratti di assistenza e manutenzione e interventi in economia

Valutazione : Accettabile

Contratto con il responsabile del trattamento

Affidamento di servizi secondo le regole del codice dei contratti

Valutazione : Accettabile

Sicurezza dell'hardware

Ordinari strumenti di sicurezza

Valutazione : Accettabile

Politica di tutela della privacy

Adeguamento dell'Ente a quanto previsto dal Regolamento UE 2016/679

Valutazione : Accettabile

Gestire gli incidenti di sicurezza e le violazioni dei dati personali

Procedura di data breach e modulistica specifica

Valutazione : Accettabile

Gestione del personale

Informativa, autorizzazione e formazione

Valutazione : Accettabile

Gestione dei terzi che accedono ai dati

Specifici contratti di servizio e relative individuazione dei responsabili del trattamento

Valutazione : Accettabile

Accesso illegittimo ai dati

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

Lesione dei diritti fondamentali dell'interessato, Danno da non corretto trattamento

Quali sono le principali minacce che potrebbero concretizzare il rischio?

errata elaborazione dei dati, accesso non autorizzato, accesso improprio di soggetti autorizzati, obsolescenza o mancato aggiornamento dei dispositivi

Quali sono le fonti di rischio?

Persone interne o esterne all'Ente malintenzionate, eventi calamitosi, quali interruzioni di corrente, incendio, inondazione, ...

Quali misure fra quelle individuate contribuiscono a mitigare il rischio?

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Vulnerabilità, Gestione postazioni, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati

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

Importante, I dati trattati sono rilevanti anche se il meccanismo di cancellazione automatica entro breve periodo, la non riconoscibilità diretta dei soggetti e le misure di protezione adottate rendono il rischio non massimo.

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

Limitata, Il meccanismo di cancellazione automatica entro breve periodo e le misure di protezione adottate rendono la probabilità non elevata.

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Modifiche indesiderate dei dati

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

Lesione dei diritti fondamentali dell'interessato, Danno da non corretto trattamento

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

errata elaborazione dei dati, accesso non autorizzato, accesso improprio di soggetti autorizzati, obsolescenza o mancato aggiornamento dei dispositivi

Quali sono le fonti di rischio?

Persone interne o esterne all'Ente malintenzionate, eventi calamitosi, quali interruzioni di corrente, incendio, inondazione, ...

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Gestione postazioni, Backup, Contratto con il responsabile del trattamento, Manutenzione, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati

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

Importante, Il rischio di modifiche indesiderate riguarda principalmente gli errati trattamenti derivanti da azione umana che potrebbero portare a conseguenti errate elaborazione di dati.

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

Limitata, Il meccanismo di cancellazione automatica entro breve periodo e le misure di protezione adottate rendono la probabilità non elevata.

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Perdita di dati

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

Lesione dei diritti fondamentali dell'interessato, Danno da non corretto trattamento, Vantaggi (omessa sanzione)

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

errata elaborazione dei dati, accesso non autorizzato, accesso improprio di soggetti autorizzati, obsolescenza o mancato aggiornamento dei dispositivi

Quali sono le fonti di rischio?

Persone interne o esterne all'Ente malintenzionate, eventi calamitosi, quali interruzioni di corrente, incendio, inondazione, ...

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

Controllo degli accessi logici, Tracciabilità, Archiviazione, Sicurezza dei documenti cartacei, Minimizzazione dei dati, Vulnerabilità, Gestione postazioni, Backup, Manutenzione, Contratto con il responsabile del trattamento, Sicurezza dell'hardware, Politica di tutela della privacy, Gestire gli incidenti di sicurezza e le violazioni dei dati personali, Gestione del personale, Gestione dei terzi che accedono ai dati

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

Massima, La gravità sarebbe massima anche se le politiche di backup consentono il recupero pressochè integrale dei dati

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

Limitata, Il meccanismo di cancellazione automatica entro breve periodo e le misure di protezione adottate rendono la probabilità non elevata.

Valutazione : Accettabile

Commento di valutazione :

Aggiornamento a seguito di incontro del gruppo di lavoro del 5 marzo 2019

Panoramica

Principi fondamentali

- Finalità
- Basi legali
- Adeguatezza dei dati
- Esattezza dei dati
- Periodo di conservazione
- Informativa
- Raccolta del consenso
- Informativa
- Diritto di rettifica e diritto di cancellazione
- Diritto di limitazione e diritto di opposizione
- Responsabili del trattamento
- Trasferimenti di dati

Misure esistenti o pianificate

- Controllo degli accessi logici
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti cartacei
- Minimizzazione dei dati
- Vulnerabilità
- Gestione postazioni
- Backup
- Manutenzione
- Contratto con il responsabile del trattamento
- Sicurezza dell'hardware
- Politica di tutela della privacy
- Gestire gli incidenti di sicurezza e le violazioni dei dati personali
- Gestione del personale
- Gestione dei terzi che accedono ai dati

Rischi

- Accesso illegittimo ai dati
- Modifiche indesiderate dei dati
- Perdita di dati

Misure Migliorabili
Misure Accettabili

Principi fondamentali

Nessun piano d'azione registrato.

Misure esistenti o pianificate

Nessun piano d'azione registrato.

Rischi

Nessun piano d'azione registrato.

Impatti potenziali

- Lesione dei diritti fondame...
- Danno da non corretto tratt...
- Vantaggi (omessa sanzione)

Minaccia

- errata elaborazione dei dati
- accesso non autorizzato
- accesso improprio di sogget...
- obsolescenza o mancato aggi...

Fonti

- Persone interne o esterne a...
- eventi calamitosi, quali in...

Misure

- Controllo degli accessi log...
- Tracciabilità
- Archiviazione
- Sicurezza dei documenti car...
- Vulnerabilità
- Gestione postazioni
- Backup
- Manutenzione
- Contratto con il responsabi...
- Sicurezza dell'hardware
- Politica di tutela della pr...
- Gestire gli incidenti di si...
- Gestione del personale
- Gestione dei terzi che acce...
- Minimizzazione dei dati

Accesso illegittimo ai dati

Gravità : Importante

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Importante

Probabilità : Limitata

Perdita di dati

Gravità : Massima

Probabilità : Limitata

Mappaggio dei rischi

