VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

ESTRATTO

Azienda/Organizzazione **Comune di Palermo**

SCHEDA 55

TITOLARE	Comune di Palermo
SEDE	Sede Istituzionale Piazza Pretoria 1, 90133 Palermo - PA

Data revisione: 01/09/2020

Sommario

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: identificazione dei trattamenti

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

In questo step è necessario raccogliere tutte le informazioni sul trattamento dei dati personali con i dettagli indicati sopra. In pratica avremo una descrizione del processo in particolare gli scopi del trattamento e le finalità di utilizzo delle informazioni personali, una descrizione delle informazioni personali coinvolte, una descrizione del contesto organizzativo interno ed esterno.
Questa fase è mirata ad avere una chiara comprensione di ciò è attualmente al fine di avere una buona base per il piano di azione che potrà permettere di definire i cambiamenti da apportare.

2° STEP: valutazione del rischio e individuazione criteri per DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio
P = probabilità di accadimento
C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	Improbabile
2	Poco probabile
3	Probabile
4	M. Probabile
5	Quasi certo

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

P r o b a b i l i t à	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico

4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – valutazione del rischio normalizzato

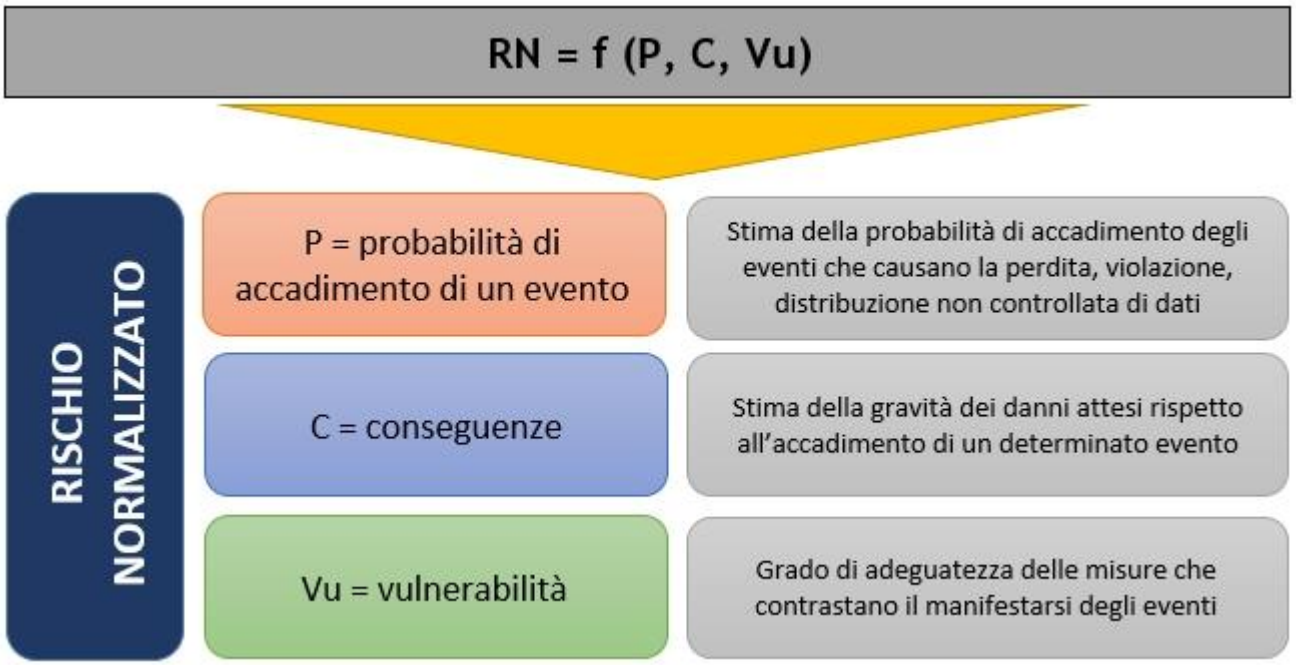
Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.
Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.
La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

RN = f (P, C, Vu)

Dove:

P = probabilità
C = conseguenze generate dall'evento
V = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il rischio intrinseco Ri come prodotto della probabilità

P e delle conseguenze C, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **probabilità P** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**Quasi certo**

Alle **conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO

Ri = P x C	Valori di riferimento
Molto basso	*(1 ≤ **Ri** ≤ 2)*
Basso	*(3 ≤ **Ri** ≤ 4)*
Rilevante	*(6 ≤ **Ri** ≤ 9)*
Alto	*(12 ≤ **Ri** ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.
Di seguito la suddivisione delle aree di pericolo con i rischi generati.

PERICOLO	RISCHI
Agenti fisici (incendio, allagamento, attacchi esterni)	• Perdita • Distruzione non autorizzata
Eventi naturali (terremoti, eruzioni vulcaniche, ecc.)	• Perdita • Distruzione non autorizzata
Interruzione servizi (sbalzi di tensione, guasti impianto di climatizzazione, interruzione collegamenti di rete, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Problemi tecnici (Anomalie e malfunzionamento software, problemi hardware o componenti servizio IT)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Compromissione informazioni (intercettazioni, rivelazione informazioni, infiltrazioni in messaggistica di posta elettronica, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato
Azioni non autorizzate (Errori volontari o involontari, virus, uso non autorizzato di strumentazione, ecc.)	• Perdita • Distruzione non autorizzata • Modifica non autorizzata • Divulgazione non autorizzata • Accesso dati non autorizzato

Per ricavare il Rischio Normalizzato RN, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.
Alla **Vulnerabilità** (Vu) è associato un indice numerico rappresentato nella seguente tabella:

VULNERABILITA'		Valore
1	Adeguate	0,25
2	Parzialmente adeguate	0,5
3	Inadeguate	1

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	1 < ***RN*** ≤ 2	3 ≤ ***RN*** ≤ 4	6 ≤ ***RN*** ≤ 9	12 ≤ ***RN*** ≤ 16
	0,5	0,5 < ***RN*** ≤ *1*	1,5 ≤ ***RN*** ≤ 2	3 < ***RN*** ≤ 5	6 ≤ ***RN*** ≤ 8
	0,25	0,25 ≤ ***RN*** ≤ 0,5	0,75 ≤ ***RN*** ≤ 1	1,5 ≤ ***RN*** < 3	3 ≤ ***RN*** ≤ 4
		1 ≤ ***Ri*** ≤ 2	3 ≤ ***Ri*** ≤ 4	6 ≤ ***Ri*** ≤ 9	12 ≤ ***Ri*** ≤ 16
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	0,25 ≤ ***RN*** ≤ 1
Basso	1 < ***RN*** < 3
Rilevante	3 ≤ ***RN*** ≤ 9
Alto	12 ≤ ***RN*** ≤ 16

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia **ALTA**, il Titolare attiva l'iter di consultazione del Garante.

Persone che sono state coinvolte o che hanno fornito consulenza:

Sono state coinvolte tutte le figure che hanno familiarità con la protezione dei dati personali e la privacy, le persone che si occupano della sicurezza delle informazioni, esperti nel settore e operatori dell'amministrazione comunale. Nello specifico le seguenti figure o settori/uffici

1. Data Protection Officer
2. Vicesegreteria Generale
3. Referenti privacy designati
4. Il dirigente del settore
5. RAP SPA

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA

- Scheda 55. Attività di Videosorveglianza

Scheda 55. Attività di Videosorveglianza

Struttura	

Personale coinvolto	
Titolare del trattamento	Comune di Palermo
Persone autorizzate	Personale autorizzato come da scheda del registro delle attività di trattamento
Partners - Responsabili esterni	RAP SPA
Altro	

Processo di trattamento	
Descrizione	Il trattamento ha per oggetto l'acquisizione di immagini e video attraverso un sistema di videosorveglianza, installato allo scopo di garantire la sicurezza del personale operante in azienda e la tutela del patrimonio strumentale aziendale. Per le sue caratteristiche di pervasività e intrusione nella sfera dei comportamenti personali, inclusa la possibilità di un controllo a distanza dei lavoratori, in osservanza al provvedimento del Garante per la Protezione dei Dati Personali dell'8 aprile 2010, e all'art.4 dello Statuto dei Lavoratori, l'azienda ha provveduto alla stipula di un accordo con le rappresentanze sindacali avente ad oggetto la puntuale regolamentazione dell'utilizzo del sistema di videosorveglianza nei locali e nelle pertinenze aziendali. Le modalità di gestione dell'impianto, l'acquisizione video, la trasmissione, la visualizzazione esclusivamente da soggetti autorizzati e formati allo scopo, l'eventuale trasmissione agli organi preposti alla pubblica sicurezza, la conservazione e la distruzione dello stesso materiale video o di immagini da esso estrapolate, si rimanda al documento approvato. iL responsabile si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto Fonti Normative • Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"; • Regolamento UE n. 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; - Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la

	decisione quadro 2008/977/GAI del Consiglio; - D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni; - art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni; - decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali; - circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471; - D.L. 23 febbraio 2009, n. 11, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", ed in particolare dall'art. 6; - "Provvedimento in materia di videosorveglianza" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.
Fonte dei dati personali	Presso l'interessato
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
Finalità del trattamento	Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione Rilevazione, prevenzione e controllo delle infrazioni Protezione della proprietà Protezione e incolumità degli individui Monitoraggio delle persone che richiedono l'accesso ai locali Attivare misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale Vigilare in materia di sicurezza urbana, sul benessere animale e/o sulla correttezza osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti Attivare uno strumento operativo di protezione civile sul territorio comunale Verificare il rispetto degli accessi in zone a traffico limitato e corsie riservate Rilevare le infrazioni al codice della strada (Monitorare la circolazione sulle strade) al fine di intervenire prontamente per prevenire ingorghi o blocchi del traffico Tutelare la sicurezza urbana Promozione turistica o pubblicitaria anche con l'utilizzo di webcam o camera on-line. In questo caso non devono essere rese visibili le persone riprese Videocontrollo ZTL inclusa validazione ed emissione verbali
Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari) Dati biometrici Personali Particolari (sensibili)
Categorie di interessati	Clienti ed utenti Cittadini
Categorie di destinatari	Società di gestione per il controllo delle frodi Autorità di vigilanza e controllo Uffici giudiziari Forze di polizia
Informativa	Si

Profilazione	Si
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Giornaliera
Termine cancellazione dati	I dati saranno conservati per il tempo strettamente necessario al perseguimento della finalità del trattamento, e, oltre, secondo i criteri suggeriti dalla normativa vigente in materia di conservazione, anche ai fini di archiviazione dei documenti amministrativi, e comunque di rispetto dei principi di liceità, necessità, proporzionalità. Si fa riferimento alla procedura di scarto degli atti di archivio allegata al registro.
Trasferimento dati (paesi terzi)	Non presente

Modalità di elaborazione dati: Informatica	
Strumenti	Software gestionale
Strutture informatiche di archiviazione	
Strutture informatiche di backup	

VALUTAZIONE DEL LIVELLO DI RISCHIO		
PROBABILITÀ	**CONSEGUENZE**	**LIVELLO DI RISCHIO**
Probabile	Gravissime	Alto

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE
OMISSIS

Contesto

Panoramica

Quale è il trattamento in considerazione?

Perché è necessario raccogliere informazioni personali?

Perché è necessario raccogliere dati particolari e/o giudiziari?

Processo di trattamento	
Descrizione	Il trattamento ha per oggetto l'acquisizione di immagini e video attraverso un sistema di videosorveglianza, installato allo scopo di garantire la sicurezza del personale operante in azienda e la tutela del patrimonio strumentale aziendale. Per le sue caratteristiche di pervasività e intrusione nella sfera dei comportamenti personali, inclusa la possibilità di un controllo a distanza dei lavoratori, in osservanza al provvedimento del Garante per la Protezione dei Dati Personali dell'8 aprile 2010, e all'art.4 dello Statuto dei Lavoratori, l'azienda ha provveduto alla stipula di un accordo con le rappresentanze sindacali avente ad oggetto la puntuale regolamentazione dell'utilizzo del sistema di videosorveglianza nei locali e nelle pertinenze aziendali. Le modalità di gestione dell'impianto, l'acquisizione video, la trasmissione, la visualizzazione esclusivamente da soggetti autorizzati e formati allo scopo, l'eventuale trasmissione agli organi preposti alla pubblica sicurezza, la conservazione e la distruzione dello stesso materiale video o di

	immagini da esso estrapolate, si rimanda al documento approvato. iL responsabile si obbliga a non effettuare riprese di dettaglio dei tratti somatici delle persone, che non siano funzionali alle finalità istituzionali dell'impianto Fonti Normative • Decreto del Presidente della Repubblica n. 15 del 15.01.2018, recante "Regolamento a norma dell'articolo 57 del decreto legislativo 30 giugno 2003, n. 196, recante l'individuazione delle modalità di attuazione dei principi del Codice in materia di protezione dei dati personali relativamente al trattamento dei dati effettuato, per le finalità di polizia, da organi, uffici e comandi di polizia"; • Regolamento UE n. 2016/679 del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE; - Direttiva UE n. 2016/680 del 27 aprile 2016 relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio; - D.Lgs. 30 giugno 2003, n, 196, recante: "Codice in materia di protezione dei dati personali" e successive modificazioni; - art. 54 del D.Lgs. 18 agosto 2000, n. 267 e successive modificazioni; - decalogo del 29 novembre 2000 promosso dal Garante per la protezione di dati personali; - circolare del Ministero dell'Interno dell'8 febbraio 2005, n. 558/A/471; - D.L. 23 febbraio 2009, n. 11, recante: "Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori", ed in particolare dall'art. 6; - "Provvedimento in materia di videosorveglianza" emanato dal garante per la protezione dei dati personali in data 8 aprile 2010.
Fonte dei dati personali	Presso l'interessato
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;
Finalità del trattamento	Difesa del suolo, tutela dell'ambiente e della sicurezza della popolazione Rilevazione, prevenzione e controllo delle infrazioni Protezione della proprietà Protezione e incolumità degli individui Monitoraggio delle persone che richiedono l'accesso ai locali Attivare misure di prevenzione e di tutela della pubblica sicurezza in ambito comunale Vigilare in materia di sicurezza urbana, sul benessere animale e/o sulla correttezza osservanza di ordinanze e/o regolamenti comunali per consentire l'accertamento dei relativi illeciti Attivare uno strumento operativo di protezione civile sul territorio comunale Verificare il rispetto degli accessi in zone a traffico limitato e corsie riservate Rilevare le infrazioni al codice della strada

	(Monitorare la circolazione sulle strade) al fine di intervenire prontamente per prevenire ingorghi o blocchi del traffico Tutelare la sicurezza urbana Promozione turistica o pubblicitaria anche con l'utilizzo di webcam o camera on-line. In questo caso non devono essere rese visibili le persone riprese Videocontrollo ZTL inclusa validazione ed emissione verbali

Quali sono le responsabilità legate al trattamento?
Chi può accedere alle informazioni personali?
È necessario condividere informazioni personali con fornitori o terze parti?

Il titolare del trattamento, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri. Inoltre, dispone tutte le attività per garantire la liceità del trattamento, infatti mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR.

Le singole responsabilità connesse al trattamento e le relative figure soggettive (Titolare - Responsabile esterno - Contitolare) sono individuate nel registro dei trattamenti.

Struttura	

Personale coinvolto	
Titolare del trattamento	Comune di Palermo
Persone autorizzate	Personale autorizzato come da scheda del registro delle attività di trattamento
Partners - Responsabili esterni	RAP SPA
Altro	

Ci sono standard applicabili al trattamento?

Non definito

Dati, processi e risorse di supporto

Quali sono i dati trattati?

Tipo di dati personali	Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali) Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari) Dati biometrici Personali Particolari (sensibili)
Categorie di interessati	Clienti ed utenti Cittadini

Categorie di destinatari	Società di gestione per il controllo delle frodi Autorità di vigilanza e controllo Uffici giudiziari Forze di polizia

Com'è il ciclo di vita del trattamento dei dati?

		CICLO DI VITA DEI DATI				
		Raccolta dei dati	Selezione e conservazione	Trattamento (uso)	Comunicazione o diffusione	Distruzione
Elementi coinvolti nelle attività di trattamento dei dati personali	Attività del processo	La raccolta avviene presso ciascuna telecamera su schede di memorizzazione crittografate	Le telecamere si accendono solo su allarme e non sono sempre attive	Verifica di eventuali abusi e attivazione del processo sanzionatorio. Accesso agli atti.	Solo nei casi previsti dalla legge e per sola comunicazione. I dati non possono essere diffusi	Sovrascrittura delle immagini entro 7 giorni. 15 giorni sui server per le immagini necessarie all'attività sanzionatoria
	Dati trattati	Immagini degli interessati	Immagini degli interessati che hanno commesso un abuso	Immagini degli interessati che hanno commesso un abuso	Immagini degli interessati che hanno commesso un abuso	Immagini degli interessati che hanno commesso un abuso
	Soggetti coinvolti	Responsabile del trattamento	Titolare del trattamento mediante i suoi incaricati designati responsabili del trattamento	Titolare del trattamento mediante i suoi incaricati designati responsabili del trattamento	Titolare del trattamento mediante i suoi incaricati designati responsabili del trattamento ed eventuali soggetti richiedenti per finalità legittime	Titolare del trattamento mediante i suoi incaricati designati responsabili del trattamento
	Tecnologie utilizzate	Registrazione su sd card con crittografia XTEA a 128 bit	Copia su un dispositivo con crittografia attiva			

Ruoli	
Interessati	Cittadini
Responsabili del Trattamento	RAP
Contitolari	

Terzi coinvolti	
Descrizione sistematica delle operazioni e finalità di trattamento	
Trasferimenti dei dati:	
Flusso dei dati tra sistemi:	
Procedura per adempiere all'obbligo di informazione, nel caso i dati vengono raccolti direttamente dall'interessato	Vengono installati i cartelli per l'informativa sulla videosorveglianza. I cartelli seguono il modello delle "Linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video"
Procedura per la richiesta del consenso, nel caso in cui i dati vengano raccolti direttamente dall'interessato (se del caso)?	Base giuridica diversa dal consenso
Procedura per l'esercizio dei diritti da parte degli interessati (accesso, rettifica, cancellazione / blocco, opposizione e portabilità)?	Tramite richiesta alla mail del protocollo comunale o del responsabile per la protezione dati personali.
Quali obblighi e misure di sicurezza sono da prevedere nei contratti con i responsabili del trattamento?	Si rimanda all'appendice C del contratto ai sensi dell'art. 28.
Nel caso in cui ci siano trasferimenti internazionali al di fuori dello spazio Economico europeo, questi sono adeguatamente protetti?	I dati non possono essere trasferiti all'estero.

Quali sono le risorse di supporto ai dati?

Le risorse su cui ospitano i dati oggetto del trattamento possono comprendere hardware, software, reti, persone, supporti cartacei o documentazione per la loro individuazione, per la loro individuazione si rimanda al Registro dei trattamenti dell'ente.

Principi Fondamentali

Proporzionalità, necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

I dati vengono raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che il trattamento non sia incompatibile con tali finalità. Un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 GDPR, in quanto considerato incompatibile con le finalità iniziali (limitazione della finalità).

Le finalità del trattamento in oggetto sono specificate ed esplicitate nelle linee stabilite dall'ente in relazione all'Attività di Videosorveglianza.
Il trattamento rispetta i principi di liceità, correttezza e trasparenza, infatti i dati personali vengono trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.
Le finalità del trattamento in oggetto e le relative basi giuridiche sono le seguenti:

- Coordinamento e direzione dell'attività di protezione civile, pronto intervento sismico e delle emergenze per tutti gli interventi calamitosi
- promozione e coordinamento nel la redazione di progetti integrati per la sicurezza
- adozione in ambito comunale delle attività di prevenzione dei rischi stabilite dai programmi e piani regionali

- attività connesse al funzionamento del Comitato Provinciale di Protezione Civile
- costituzione di COC e gestione della sala radio operativa del Comune e delle relative funzioni di supporto di emergenza ai COM e CCS
- iniziative di formazione e informazione in materia di Protezione Civile e di educazione alla sicurezza
- Gestione e coordinamento del Gruppo Comunale dei Volontari della Protezione Civile per la programmazione e l'attuazione di attività e servizi ordinari
- Predisposizione e gestione delle esercitazioni comunali per la struttura comunale e per il gruppo di volontari in materia di Protezione Civile per i grandi rischi
- Adozione di tutti i provvedimenti, compresi quelli relativi alla preparazione all'emergenza, necessari ad assicurare i primi soccorsi in caso di eventi calamitosi
- Attivazione dei primi soccorsi alla popolazione e degli interventi urgenti necessari a fronteggiare l'emergenza
- Attuazione degli interventi di somma urgenza per la salvaguardia della pubblica incolumità derivante da eventi calamitosi
- Attuazione in ambito comunale delle attività di previsione dei rischi stabiliti dai programmi e piani regionali
- Fare eseguire, successivamente alla notifica delle ordinanze (effettuata d'intesa con il Servizio Messi), gli interventi per l'eliminazione degli immediati pericoli per la pubblica incolumità
- Organizzare i necessari rapporti con i servizi pubblici competenti in materia di pronto soccorso, salvataggio, lotta antincendio e gestione dell'emergenza
- Pianificazione e gestione degli interventi di protezione civile e relazione con le organizzazioni di protezione civile
- Predisposizione dei piani comunali e/o intercomunali di emergenza in base a degli indirizzi regionali
- Servizio di pronta reperibilità per gli interventi da effettuare in materia
- Vigilanza sull'attuazione, da parte delle strutture locali di protezione civile, dei servizi urgenti. Utilizzo del volontariato di protezione civile
- Coordinamento del Servizio di pronta reperibilità dell'Amministrazione in raccordo con il dirigente delle funzioni tecniche aventi personale in reperibilità e gestione per gli interventi da effettuare in materia

Quali sono le basi legali che rendono il trattamento legittimo?

Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	trattamento è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	Il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri, che deve essere proporzionato alla finalità perseguita, rispettare l'essenza del diritto alla protezione dei dati e prevedere misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato;

L'utilizzo dei sistemi di videosorveglianza è espressamente previsto nel caso di monitoraggio e

accertamento dell'uso abusivo di aree impiegate a discarica e deposito rifiuti. Avendo il comune comunque tentato una serie di misure che sono risultate inefficaci, si ritiene che l'installazione delle telecamere sia lecita.

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

Una efficace tutela della privacy è quella di raccogliere le informazioni strettamente necessarie al progetto in questione. I dati vengono raccolti perché esistono leggi e regolamenti specifici che consentono di raccogliere i dati.

La raccolta dei dati viene effettuata nel rispetto del Principio di Minimizzazione dei dati, ovvero si svolge in maniera tale da ridurre la gravità dei rischi limitando la raccolta di dati personali al minimo necessario per la specifica finalità. Evitare di raccogliere dati non necessari, di utilizzare dati che non abbiano alcun rapporto con la specifica finalità e di produrre impatti eccessivi sulle persone. I dati raccolti sono necessari per il raggiungimento delle finalità, nello specifico si richiedono i seguenti dati personali: Dati sul comportamento (creazione di profili di utenti, consumatori, contribuenti, ecc.; profili della personalità e dei tratti caratteriali); Abitudini di vita o di consumo (viaggi, spostamenti, preferenze o esigenze alimentari); Dati biometrici; Personali; Particolari (sensibili).

I dati sono accurati e mantenuti aggiornati?

Ai sensi dell'art. 5 comma 1 lett. d) GDPR, i dati trattati sono esatti e, se necessario, aggiornati. Inoltre, vengono adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.

Quale è la durata della conservazione dei dati?

I dati saranno conservati per il tempo strettamente necessario al perseguimento della finalità del trattamento, e, oltre, secondo i criteri suggeriti dalla normativa vigente in materia di conservazione, anche ai fini di archiviazione dei documenti amministrativi, e comunque di rispetto dei principi di liceità, necessità, proporzionalità. Si fa riferimento alla procedura di scarto degli atti di archivio allegata al registro.

I dati sulla videosorveglianza comunale possono essere raccolti per un massimo di 7 giorni con attivazione automatica della sovrascrittura e verifica periodica, almeno ogni 6 mesi, dell'efficacia dell'operazione di cancellazione.

Controlli per proteggere i diritti personali dei soggetti interessati

Controlli

L'elenco completo dei controlli è disponibile nella scheda "Valutazione della sicurezza". Le misure di sicurezza possono variare a secondo dell'impianto in uso ma alcuni possono essere considerati controlli "minimi" inderogabili e sono elencati di seguito:

a) le differenti e specifiche competenze devono essere attribuite ai singoli operatori con diversi livelli di

accesso per la visione e il trattamento delle immagini;

b) per i sistemi predisposti per la registrazione e la conservazione delle immagini rilevate, limitare, anche ai soggetti abilitati, la possibilità di visionare contestualmente alla ripresa, o successivamente, le immagini registrate e di duplicarle o cancellarle;

c) le immagini memorizzate devono essere cancellate, in forma automatica, allo scadere del termine previsto di 7 giorni mediante sovrascrittura automatica. Questo controllo deve essere verificato periodicamente e almeno ogni sei mesi.

Per i comuni e nelle sole ipotesi in cui l'attività di videosorveglianza urbana o ambientale, sia finalizzata alla tutela della sicurezza urbana, il termine massimo di durata per la conservazione dei dati è limitato "ai sette giorni successivi alla rilevazione delle informazioni e delle immagini raccolte mediante l'uso di sistemi di videosorveglianza, fatte salve speciali esigenze di ulteriore conservazione;

d) nel caso di interventi di manutenzione delle apparecchiature, devono essere adottate specifiche cautele; in particolare, ai soggetti addetti alla manutenzione deve essere consentito di accedere alle immagini solo per indispensabili verifiche tecniche e in presenza dei soggetti con credenziali di autenticazione abilitanti alla visione delle immagini;

e) nelle ipotesi di utilizzo di apparecchiature di ripresa digitali connesse a reti informatiche, proteggere gli apparati contro i rischi di accesso abusivo (art. 615 ter Codice penale);

f) solo nel caso di effettuare la trasmissione di immagini riprese con apparati di videosorveglianza, tramite rete pubblica, con tecniche crittografiche che ne garantiscano la riservatezza. Le stesse cautele sono richieste per la trasmissione delle immagini dai punti di ripresa dotati di connessioni wireless.

g) per gli impianti che non trasmettono in real time le immagini è necessario configurare le schede di registrazione mediante criptazione adeguata e conforme allo stato attuale delle tecnologie.

I soggetti interessati come sono informati del trattamento?

Agli interessati verranno fornite tutte le informazioni inerenti al trattamento in oggetto. Nello specifico verranno indicati i contatti del Titolare del trattamento e del Responsabile per al protezione dei dati personali (DPO); le finalità del trattamento, la natura del conferimento; le modalità del trattamento; le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o Incaricati; le basi giuridiche che legittimano il procedimento e i diritti dell'interessato. Gli interessati sono informati del trattamento tramite informativa ai sensi dell'art 13 e 14 GDPR allegata al modulo di richiesta del contributo economico.

Come si ottiene il consenso dei soggetti interessati?

Nessuna delle finalità prevede la richiesta di consenso.

I soggetti interessati come esercitano i loro diritti di acceso alla portabilità dei dati?

L'interessato ha diritto 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 personali (art. 15 GDPR).

L'interessato non ha il diritto di ottenere la portabilità dei dati.

La richiesta di esercizio del diritto può essere effettuata, facendo richiesta alla mail del dpo: rpd@comune.palermo.it ovvero alla seguente e-mail: protocollo@cert.comune.palermo.it. Sono in corso sperimentazioni per una procedura più strutturata come indicato nel verbale del 18-19-20 Ottobre 2019 e negli audit di Luglio 2019.

Eventuali diritti di accesso sono esercitabili così come disciplinato dalla legislazione vigente e secondo il regolamento comunale sulle modalità di esercizio del diritto di accesso.

Come i soggetti interessati esercitano i loro diritti alla rettifica e alla cancellazione?

L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; l'interessato si oppone al trattamento; i dati personali sono stati trattati illecitamente; i dati personali devono essere cancellati per adempiere un obbligo legale previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento.

La richiesta di esercizio del diritto può essere effettuata, facendo richiesta alla mail del dpo: rpd@comune.palermo.it ovvero alla seguente e-mail: protocollo@cert.comune.palermo.it. Sono in corso sperimentazioni per una procedura più strutturata come indicato nel verbale del 18-19-20 Ottobre 2019 e negli audit di Luglio 2019.

Lo specifico trattamento non è soggetto al diritto di rettifica.

i soggetti interessati come esercitano il loro diritto di restrizione e obiezione?

L'interessato ha il diritto di ottenere dal titolare del trattamento la limitazione del trattamento, ex art. 18 del [GDPR], inoltre ha il diritto di opporsi in qualsiasi momento, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano in conformità con l'art. 21 del [GDPR].

Ad ogni modo, gli interessati esercitano i diritti descritti attenendosi a quanto disposto dalla Politica di sicurezza in caso di reclami e incidenti relativi alla privacy adottata dal Titolare. La richiesta di esercizio del diritto può essere effettuata, facendo richiesta alla mail del dpo: rpd@comune.palermo.it ovvero alla seguente e-mail: protocollo@cert.comune.palermo.it. Sono in corso sperimentazioni per una procedura più strutturata come indicato nel verbale del 18-19-20 Ottobre 2019 e negli audit di Luglio 2019

Gli obblighi dei responsabili del trattamento sono chiaramente identificati e governati da un contratto?

Gli obblighi dei responsabili del trattamento vengono descritti e definiti in ambito di sottoscrizione del contratto generale e del contratto speciale sulla protezione dei dati.

Nel caso di trasferimento di dati fuori dall'Unione Europea, i dati sono adeguatamente protetti?

I dati non vengono mai trasferiti al di fuori dell'Unione Europea

Rischi

Controlli esistenti o pianificati

Idealmente, un PIA identificherà sia i rischi per l'individuo, e le opportunità per l'organizzazione di beneficiare di una migliore e più efficace protezione dei dati personali. Mentre questa sezione si concentra sulla identificazione e la mitigazione dei rischi, l'action plan cercherà di utilizzare questa analisi per identificare e massimizzare le opportunità.

Che cosa è un rischio per la privacy?

Un "rischio privacy" è il rischio che il trattamento non riuscirà ad avere ragionevoli aspettative di mantenere privacy e protezione dei dati degli interessati coinvolti - ad esempio perché apre un problema legale, o si intromette in maniera irragionevole nel loro spazio personale, o è in contrasto con ciò che il rapporto con gli interessati dovrebbe fare.

Calcolare il rischio non è semplicemente valutare se il progetto sarà conforme alla legge. E 'possibile rispettare la legge e ma comunque influenzare negativamente le aspettative dei cittadini sulla loro privacy. La natura del trattamento può suggerire che si dovrebbe dare una protezione ancora migliore di quanto la legge richiede. I principi forniscono un buon quadro di riferimento facendosi le domande giuste - sia legale che non legali - circa l'impatto sugli interessati.

I rischi per un individuo spesso sono equiparati a rischi per l'organizzazione.

Verranno presi in considerazione non solo i rischi diretti, ma anche qualsiasi effetto consequenziale.

Il primo rischio valutato è la possibilità di perdita dei dati dovuti al furto delle schede sd dove sono memorizzate le immagini degli interessati.

Un secondo rischio da valutare è la possibilità di gestione dei dati sul server dell'amministrazione comunale per la verifica degli abusi.

Un terzo rischio è la possibilità di diffusione delle immagini degli abusivi o la comunicazione a soggetti non autorizzati.

RISCHI IDENTIFICATI PER IL TRATTAMENTO

Questa tabella dei rischi ha lo scopo di aiutare a identificare, descrivere e gestire i potenziali rischi per i dati personali coinvolti nel progetto.

PRIORITÀ DEI RISCHI

Una tabella dei rischi consente di assegnare priorità ai rischi in base alla probabilità (verosimiglianza) che si concretizzino le minacce e di valutare la gravità dei loro potenziali impatti. È quindi possibile decidere quali controlli sono più necessari.

IDENTIFICAZIONE DEI CONTROLLI

In questa fase sono stati identificati i controlli necessari che possono aiutare l'organizzazione a funzionare in modo più efficiente. L'uso appropriato di strumenti e tecnologie per il miglioramento della privacy può contribuire a ridurre i potenziali effetti negativi in diversi modi e può ridurre o eliminare la necessità di altre misure di salvaguardia.