C O M U N E D I V E N T I C A N O

Provincia di Avellino

DATA PROTECTION IMPACT ASSESSMENT

VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI

(art.35 Regolamento UE/2016/679 GDPR)

-Ver.1.0 del 10/05/2021-

Realizzata da:
DPO
Ing antonio lubrano lavadera

INDICE

PARTE IV

PARTE V

PARTE VI

PARTE I-Premessa

Normativa di riferimento

Ai fini della redazione del presente atto di fa riferimento specificatamente ai seguenti atti normativi:

- Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio, 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 (regolamento generale sulla protezione dei dati);

- Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali" come modificato e integrato dal Decreto Legislativo 10 agosto 2018 n.101;

- Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15. 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;

- European Data Protection Board Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, adottate nel luglio 2019 dal Comitato Europeo per la Protezione dei Dati (EDPB) e aggiornate peraltro nella relase 2.0 il 29 gennaio 2020;

- Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) [Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679 Versione adottata l'11 aprile 2018];

- Decreto Legislativo 18 agosto 2000, n. 267. Testo unico delle leggi sull'ordinamento degli enti locali.

PARTE II-INQUADRAMENTO DELLA DPIA

Lo scopo della valutazione d'impatto o DPIA

La valutazione d'impatto è una procedura, nota anche con l'acronimo DPIA (Data Protection Impact Assessment) o PIA (Privacy Impact Assessment), come si indicherà nel seguito, è prevista dall'articolo 35 del Regolamento UE/2016/679 (GDPR) e ha lo scopo di descrivere un trattamento di dati per valutarne la necessità e la proporzionalità così come tutti gli altri principi fondamentali del GDPR.

Il processo di PIA può riguardare un singolo trattamento anche più trattamenti che presentino analogie per natura, ambito, finalità e rischi[1].

Dalla descrizione del trattamento ne consegue la valutazione e quindi la predisposizione di idonee misure per affrontarlo.

La PIA è uno strumento importante in termini di responsabilizzazione (accountability) in quanto aiuta il titolare a rispettare le prescrizioni normative ma attesta anche di aver adottato idonee misure per garantirne il rispetto.

Obbligo della PIA

1.L'OBBLIGO SECONDO LE PRESCRIZIONI DEL GDPR.

Il PIA (Privacy Impact Assessment) è obbligatorio in tutti i casi previsti dall'articolo 35 comma 1 del Reg.UE 2016/679 GDPR[2] ossia quando un trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche e questo può avvenire per varie ragioni:

- per l'implementazione di nuove tecnologie;
- a causa della natura, dell'oggetto, del contesto o delle finalità del trattamento.

Lo stesso articolo 35 del Reg.UE 2016/679 GDPR al comma 3[3] cita anche alcune ipotesi specifiche che rendono sempre obbligatoria la PIA che sono:

- la 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 (art.35 c.3 p.a GDPR);

[1] Regolamento UE/2016/679 GDPR, art.35 c.1 "…Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi…".

[2] Reg.UE/2016/679 GDPR, articolo 35 (Valutazione d'impatto sulla protezione dei dati) "1. Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, …".

[3] Reg.UE/2016/679 GDPR, art.35 c.3 "La valutazione d'impatto sulla protezione dei dati di cui al paragrafo 1 è richiesta in particolare nei casi seguenti: 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; o c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.".

- 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 (art.35 c.3 p.b GDPR);
- la sorveglianza sistematica su larga scala di una zona accessibile al pubblico (art.35 c.3 p.c GDPR).

2.L'ESCLUSIONE DELLA NECESSITÀ DELLA PIA SECONDO LE PRESCRIZIONI DEL GDPR.

Lo stesso articolo 35 del Reg. UE 2016/679 GDPR al punto 10[4] stabilisce che il PIA è esclusa quando si verificano contemporaneamente le seguenti condizioni:

1. Finalità del trattamento di interesse pubblico e specificatamente in uno dei seguenti casi:
   a. per adempiere un obbligo legale al quale è soggetto il titolare del trattamento;
   b. per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento.

2. Disciplina normativa esplicita della finalità di interesse pubblico contenuta in un atto normativo Europeo o dello Stato membro al quale il titolare del trattamento è soggetto.

3. Sia già stata eseguita una PIA nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione della disciplina giuridica di cui al punto precedente.

3.GLI ULTERIORI OBBLIGHI DI PIA INTRODOTTI DAL GARANTE PER LA PRIVACY.

Il GDPR ha previsto espressamente che l'Autorità Nazionale di controllo ha il potere e la facoltà di prevedere delle specifiche tipologie di trattamento per i quali è obbligatoria l'adozione del PIA (art.35 c.4 GDPR)[5]. In questi casi costei ha l'obbligo di pubblicare il provvedimento e comunicarlo al comitato europeo per la protezione dei dati (art.35 c.6 GDPR)[6] che era Gruppo di lavoro art.29 o Working Party article 29 (noto anche con l'acronimo WP29). Questa prassi doveva adottarsi fino al 25 maggio del 2018 (data di entrata in vigore del RGPD) e aveva lo scopo di occuparsi di questioni relative alla protezione della vita privata e dei dati personali. Esso, successivamente, è stato sostituito dal Comitato Europeo per la protezione dei dati (art.68 GDPR).

Per specificare nel dettaglio e dare maggiore certezza è intervenuto il provvedimento del Garante per la Protezione dei Dati Personali che con la delibera 11 ottobre 2018, n.467 "*Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati, ai sensi dell'articolo 35, comma 4, del regolamento (UE) n. 2016/679*", che ha attuato le indicazioni del

---

[4] Reg.UE/2016/679 GDPR, art.35 c.10 "Qualora il trattamento effettuato ai sensi dell'articolo 6, paragrafo 1, lettere c) o e), trovi nel diritto dell'Unione o nel diritto dello Stato membro cui il titolare del trattamento è soggetto una base giuridica, tale diritto disciplini il trattamento specifico o l'insieme di trattamenti in questione, e sia già stata effettuata una valutazione d'impatto sulla protezione dei dati nell'ambito di una valutazione d'impatto generale nel contesto dell'adozione di tale base giuridica, i paragrafi da 1 a 7 non si applicano, salvo che gli Stati membri ritengano necessario effettuare tale valutazione prima di procedere alle attività di trattamento.".

[5] Reg.UE/2016/679 GDPR, art.35 c.4 "L'autorità di controllo redige e rende pubblico un elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati ai sensi del paragrafo 1. L'autorità di controllo comunica tali elenchi al comitato di cui all'articolo 68.".

[6] Reg.UE/2016/679 GDPR, art.35 c.6 "Prima di adottare gli elenchi di cui ai paragrafi 4 e 5, l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione.".

Working Party article 29 del 2017 fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018.

In questo modo si è stabilito l'obbligo di PIA nei casi in cui ricorrano almeno due di questi criteri anche se il titolare può deciderla anche quando ne ricorra uno solo in funzione delle implicazioni sulla sicurezza:

- trattamenti valutativi o di scoring, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es. assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es. videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es. informazioni sulle opinioni politiche);
- trattamento di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per differenti finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene ad esempio con i big data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es. riconoscimento facciale, devices Internet of Things, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es. screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

4.I CASI DI ESCLUSIONE DELLA PIA STABILITI DAL GARANTE PER LA PRIVACY.

Il Garante per la Protezione dei Dati Personali, secondo quanto previsto dal Regolamento Europeo (art.35 c.5 GDPR)[7], ha stabilito che il PIA non è necessario per i trattamenti che:

- non presentano rischio elevato per i diritti e le libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata svolta una PIA;
- sono stati già sottoposti a verifica da parte di un'autorità di controllo prima del maggio 2018 e le cui condizioni (es. oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo del trattamento per i quali non è necessaria provvedere alla PIA;
- fanno riferimento a norme o regolamenti, Ue o di uno Stato membro, per la cui definizione è stata condotta una PIA.

Chi deve svolgere la PIA

Il titolare del trattamento ha la responsabilità di valutare la necessità del Privacy Impact Assessment (art.35 c.2 GDPR)[8] e, laddove si renda necessaria, l'obbligo di provvedere alla sua realizzazione

[7] Reg.UE/2016/679 GDPR, art.35 c.5 "L'autorità di controllo può inoltre redigere e rendere pubblico un elenco delle tipologie di trattamenti per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati. L'autorità di controllo comunica tali elenchi al comitato.".

[8] Reg.UE/2016/679 GDPR, art.35 c.2 "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.".

sovrintendendo sempre ogni fase pur se la realizzazione materiale sia demandata ad altro soggetto (consulente esterno o dipendente).

Nella decisione sulla realizzazione e nello svolgimento si consulta con il DPO/RDP (Data protection officer/Responsabile per la protezione dei dati). Inoltre, se il trattamento lo richiede, può acquisire pareri di esperti, tecnici e in particolare del responsabile della sicurezza dei sistemi informativi (noto anche come Chief Information Security Officer, acronimo CISO) e del responsabile IT (acronimo di Information Technology), laddove presenti, da allegare alla PIA.

Se lo ritiene necessario, il Titolare può acquisire anche il parere degli interessati o dei loro rappresentanti purché ciò non pregiudichi gli interessi dell'Ente e purché non si mettano a rischio i trattamenti stessi che si vogliono valutare con la PIA (art.35 c.9 GDPR)[9].

Aggiornamento del PIA

Il PIA non è un documento statico, ma proprio per le sue finalità generali, richiede un processo costante di verifica ed eventuale aggiornamento perlomeno quando insorgono variazioni del rischio, secondo il contesto e le evoluzioni tecnologiche, ovvero mutino o si evolvano le attività relative al trattamento.

In questi casi il titolare del trattamento procede a un riesame per valutare se dalle variazioni delle procedure del trattamento che sono intervenute e/o dalle mutate condizioni del contesto ne scaturisca un pregiudizio, anche solo potenziale, sulla sicurezza del trattamento dei dati personali e se le previsioni contenute nel PIA siano ancora valide e attuali (art.35 c.11 GDPR)[10].

I principi di valutazione del trattamento

La valutazione della PIA deve uniformarsi ai valori e ai criteri generali del trattamento dei dati contenuti nel GDPR e in particolare verificare che siano attuati i principi di:

- liceità, correttezza e trasparenza (art.5 c.1 p.a GDPR);
- limitazione delle finalità (art.5 c.1 p.b GDPR);
- minimizzazione dei dati (art.5 c.1 p.c GDPR);
- esattezza (art.5 c.1 p.d GDPR);
- diritto all'oblio (art.5 c.1 p.e GDPR);
- integrità e riservatezza (art.5 c.1 p.f GDPR);
- responsabilizzazione (art.5 c.2 GDPR).

1.LICEITÀ, CORRETTEZZA E TRASPARENZA.

L'articolo 5 comma 1 punto a) del GDPR[11] impone che i dati personali siano sempre trattati in modo lecito, corretto e trasparente nei confronti dell'interessato.

---

[9] Reg.UE/2016/679 GDPR, art.35 c.9 "Se del caso, il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.".

[10] Reg.UE/2016/679 GDPR, art.35 c.11 "Se necessario, il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento.".

[11] Reg.UE/2016/679 GDPR, articolo 5 (Principi applicabili al trattamento di dati personali) c.1 p. a): "1. I dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»)…".

Il principio di correttezza va a sostituire il principio di lealtà precipuo della vecchia normativa nella quale dominava un rapporto tra il titolare e l'interessato mentre oggi l'impegno è esteso all'intera società nella quale tutti noi viviamo e esplichiamo i nostri diritti e doveri, per cui il trattamento deve essere corretto, così garantendo all'intera collettività che il trattamento non ponga a rischio i dati personali.

La definizione del principio di correttezza è stata formulata già dal Gruppo di lavoro art.29 o Working Party article 29 (noto anche con l'acronimo WP29), sostituito oggi dall'European Data Protection Board (noto anche con l'acronimo EDPB), che è il gruppo di lavoro comune delle autorità nazionali di vigilanza e protezione dei dati, con riferimento alla chiarezza e trasparenza delle informative, sostenendo la necessità che l'informazione fornita all'interessato debba essere tale da far comprendere in modo adeguato, "le modalità con cui i dati sono raccolti, utilizzati e consultati grazie ad informazioni e comunicazioni facilmente accessibili e comprensibili, utilizzando un linguaggio semplice e chiaro" (art.12 c.1 GDPR)[12] e anche le conseguenze.

Quindi, il principio di liceità e correttezza è funzionale e rafforzativo dell'obbligo di trasparenza del trattamento nei confronti degli interessati che rappresenta un vero e proprio diritto dell'interessato.

Il punto di partenza della PIA è la valutazione della documentazione complessiva relativa al trattamento dei dati e in particolare dell'informativa resa agli interessati.

2.LIMITAZIONE DELLE FINALITÀ.

L'articolo 5 comma 1 punto b del GDPR[13] stabilisce che i dati personali siano raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità, quindi secondo un principio generale di necessità e proporzionalità che deve applicarsi a tutte le informazioni relative alle persone fisiche e quindi la valutazione della PIA deve escludere che possano esserci dei trattamenti indiscriminati.

Il titolare del trattamento deve stabilire quindi, prima dell'inizio del trattamento, in maniera precisa e tassativa evitando formulazioni generiche o illimitate, gli scopi in base ai quali ha intenzione di raccogliere e trattare i dati personali e deve limitarsi alle finalità che ha comunicato all'interessato prima dell'inizio della raccolta dei dati e quindi del trattamento.

Ciò implica che se alcuni dei dati personali o se i dati personali di alcuni soggetti non servono per le finalità del trattamento, essi non devono neppure essere raccolti e la PIA deve quindi verificare che ciò non avvenga nel processo dell'intero trattamento.

---

[12] Reg.UE/2016/679 GDPR, articolo 12 (Informazioni, comunicazioni e modalità trasparenti per l'esercizio dei diritti dell'interessato): "*1. Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori. Le informazioni sono fornite per iscritto o con altri mezzi, anche, se del caso, con mezzi elettronici. Se richiesto dall'interessato, le informazioni possono essere fornite oralmente, purché sia comprovata con altri mezzi l'identità dell'interessato. …".*

[13] Reg.UE/2016/679 GDPR, art.5 c.1 p.b): "*1. I dati personali sono: …b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che 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, considerato incompatibile con le finalità iniziali («limitazione della finalità...*".

3.MINIMIZZAZIONE DEI DATI.

Il principio di minimizzazione dei dati parte dall'idea fondamentale che il titolare deve trattare solo i dati di cui ha realmente bisogno per raggiungere le finalità del trattamento, pertanto l'articolo 5 comma 1 punto c del GDPR[14] impone che i dati personali oggetto di trattamento abbiano le caratteristiche di:

- adeguatezza, vale a dire proporzionalità rispetto alle finalità per la quale sono raccolti;
- pertinenza rispetto alle finalità precedentemente definite;
- limitazione a quanto necessario al raggiungimento delle finalità per i quali sono trattati.

Dunque i dati raccolti devono essere adeguati e pertinenti rispetto al fine che si intende perseguire, ed essi non possono essere raccolti in misura maggiore a quella necessaria.

In sostanza si stabilisce l'obbligo di verificare che per le esigenze del trattamento siano raccolti e gestiti il minor quantitativo di dati possibili.

La PIA, per questo fine, deve conoscere l'estensione dei trattamenti e valutare l'effettiva necessità dell'estensione della base di dati trattati rispetto alle finalità.

4. ESATTEZZA DEI DATI.

L'articolo 5 comma 1 punto d del GDPR[15] impone che i dati trattati devono essere esatti e, se necessario, aggiornati.

Il titolare, inoltre, deve prendere tutte le misure ragionevoli per cancellare o rettificare tempestivamente quelli che non sono più esatti e, laddove non rilevi errori di sua iniziativa, l'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo e, tenuto conto delle finalità del trattamento, può chiedere anche l'integrazione dei dati personali incompleti fornendo, eventualmente, una dichiarazione integrativa (art.16 GDPR)[16].

La PIA, a questo scopo, deve verificare le misure e i sistemi di verifica sulla correttezza dei dati.

5. DIRITTO ALL'OBLIO.

Il diritto all'oblio, inizialmente riconosciuto soltanto a livello giurisprudenziale sia in campo europeo che nazionale, può essere definito come l'interesse di un singolo ad essere dimenticato e consiste, quindi, nell'obbligo automatico di eliminazione dei trattamenti quando vengono meno la finalità per cui sono trattati, è espressamente riconosciuto dall'articolo 17 del GDPR quando si verifichino le seguenti condizioni[17]:

---

[14] Reg.UE/2016/679 GDPR, art.5 c.1 p.c): "1. I dati personali sono: … c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); …".

[15] Reg.UE/2016/679 GDPR, art.5 c.1 p.d): "1. I dati personali sono: …d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); …".

[16] Reg.UE/2016/679 GDPR, articolo 16 (Diritto di rettifica): "1.L'interessato ha il diritto di ottenere dal titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.".

[17] Reg.UE/2016/679 GDPR, articolo 17 (Diritto alla cancellazione-«diritto all'oblio»): "1. L'interessato ha il diritto di ottenere dal titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo e il

1. i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati (art.17 c.1 p.a GDPR);
2. l'interessato revoca il consenso su cui si basa il trattamento (art.17 c.1 p.b GDPR);
3. l'interessato si oppone al trattamento nei casi previsti (art.17 c.1 p.c GDPR);
4. i dati personali sono stati trattati illecitamente (art.17 c.1 p.d GDPR);
5. sussiste un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro per cancellare i dati personali (art.17 c.1 p.e GDPR);
6. i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione (art.17 c.1 p.f GDPR).

In tutti questi casi il titolare del trattamento è obbligato a cancellare ogni dato, anche quelli resi eventualmente pubblici secondo la tecnologia disponibile, e in questi casi informerà anche gli altri titolari del trattamento che siano in possesso dei dati personali degli interessati che hanno richiesto la cancellazione affinché provvedano a eliminare i propri trattamenti e cancellino qualsiasi link o copia[18].

L'articolo 5 comma 1 punto e del GDPR[19] impone l'obbligo di eliminare o, nei casi previsti, di rendere anonimi i trattamenti nell'esatto momento in cui essi non sono più giustificati secondo i principi che si sono indicati in precedenza, pertanto il procedimento oggetto della verifica PIA deve valutare che sussista un sistema automatizzato che, prescindendo dalla richiesta dell'interessato e/o dalla revoca del consenso, laddove esso sia il fondamento giuridico del trattamento, elimini il trattamento quando si verifichino queste condizioni.

L'eliminazione può essere sostituita dall'anomizzazione dei dati per scopi di archiviazione nel pubblico interesse, di ricerca scientifica o storica ovvero a fini statistici.

Il diritto all'oblio è espressamente escluso in casi tassativamente previsti e specificatamente quando il trattamento si rende necessario:

1. per l'esercizio del diritto alla libertà di espressione e di informazione (art.17 c.3 p.a GDPR)[20];

---

titolare del trattamento ha l'obbligo di cancellare senza ingiustificato ritardo i dati personali, se sussiste uno dei motivi seguenti: a) i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; b) l'interessato revoca il consenso su cui si basa il trattamento conformemente all'articolo 6, paragrafo 1, lettera a), o all'articolo 9, paragrafo 2, lettera a), e se non sussiste altro fondamento giuridico per il trattamento; c) l'interessato si oppone al trattamento ai sensi dell'articolo 21, paragrafo 1, e non sussiste alcun motivo legittimo prevalente per procedere al trattamento, oppure si oppone al trattamento ai sensi dell'articolo 21, paragrafo 2; d) i dati personali sono stati trattati illecitamente; e) i dati personali devono essere cancellati per adempiere un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento; f) i dati personali sono stati raccolti relativamente all'offerta di servizi della società dell'informazione di cui all'articolo 8, paragrafo 1. ….".

[18] Reg.UE/2016/679 GDPR, art.17 c.2: "2. Il titolare del trattamento, se ha reso pubblici dati personali ed è obbligato, ai sensi del paragrafo 1, a cancellarli, tenendo conto della tecnologia disponibile e dei costi di attuazione adotta le misure ragionevoli, anche tecniche, per informare i titolari del trattamento che stanno trattando i dati personali della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali. ….".

[19] Reg.UE/2016/679 GDPR, art.5 c.1 p.e): "1. I dati personali sono: …e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»);…".

[20] Reg.UE/2016/679 GDPR, art.17 c.3 p.a: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: a) per l'esercizio del diritto alla libertà di espressione e di informazione".

2. per l'adempimento di un obbligo giuridico previsto dal diritto dell'Unione o dello Stato membro o per l'esecuzione di un compito svolto nel pubblico interesse o nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento (art.17 c.3 p.b GDPR)[21]; ;
3. per motivi di pubblico interesse nella sanità pubblica (art.17 c.3 p.c GDPR)[22]; ;
4. a fini di archiviazione e di statistica nel pubblico interesse, di ricerca scientifica o storica (art.17 c.3 p.d GDPR)[23];
5. in ambito giudiziario per l'esercizio o la difesa di un diritto (art.17 c.3 p.e GDPR)[24]; .

6.PRINCIPIO DI INTEGRITÀ E RISERVATEZZA.

Il principio di integrità e riservatezza è previsto dall'articolo 5 comma1 punto f del GDPR[25] e stabilisce che i dati devono essere sempre trattati in modo da garantirne una sicurezza adeguata.

Il titolare del trattamento ha l'obbligo quindi di adottare tutte le misure di sicurezza tecniche e organizzative adeguate al fine di proteggere i dati stessi da trattamenti non autorizzati o illeciti, dalla loro sottrazione, perdita, distruzione, danni accidentali, ossia da tutte quelle ipotesi che configurerebbero un data breach (art.34 GDPR)[26].

La PIA quindi deve verificare preventivamente che la sicurezza sia garantita nei confronti dei dati lungo l'intero ciclo del trattamento e, laddove non sia possibile eliminare del tutto il rischio che siano adottate tutte le misure disponibili, sul piano fisico e tecnologico, per minimizzare il rischio.

7.PRINCIPIO DI RESPONSABILITÀ.

Il principio di accountability previsto nel testo originale del GDPR approvato in lingua inglese, previsto dall'articolo 5 comma 2 del GDPR[27], è stato tradotto come "responsabilizzazione" e definito

---

[21] Reg.UE/2016/679 GDPR, art.17 c.3 p.b: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: … b) per l'adempimento di un obbligo giuridico che richieda il trattamento previsto dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento o per l'esecuzione di un compito svolto nel pubblico interesse oppure nell'esercizio di pubblici poteri di cui è investito il titolare del trattamento;…".

[22] Reg.UE/2016/679 GDPR, art.17 c.3 p.c: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: …c) per motivi di interesse pubblico nel settore della sanità pubblica in conformità dell'articolo 9, paragrafo 2, lettere h) e i), e dell'articolo 9, paragrafo 3;…".

[23] Reg.UE/2016/679 GDPR, art.17 c.3 p.d: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: …d) a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici conformemente all'articolo 89, paragrafo 1, nella misura in cui il diritto di cui al paragrafo 1 rischi di rendere impossibile o di pregiudicare gravemente il conseguimento degli obiettivi di tale trattamento;…".

[24] Reg.UE/2016/679 GDPR, art.17 c.3 p.e: "I paragrafi 1 e 2 non si applicano nella misura in cui il trattamento sia necessario: …e) per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.".

[25] Reg.UE/2016/679 GDPR, art.5 c.1 p.f): "1. I dati personali sono:…f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)…".

[26] Reg.UE/2016/679 GDPR, articolo 34 (Notifica di una violazione dei dati personali all'autorità di controllo): "1. In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

[27] Reg.UE/2016/679 GDPR, art.5 c.2: "Il titolare del trattamento è competente per il rispetto del paragrafo 1 e in grado di comprovarlo («responsabilizzazione»).".

come l'obbligo posto in capo al titolare del trattamento di essere competente, e quindi concretamente in grado, di garantire i principi generali del trattamento indicati in precedenza e altresì di poterlo comprovare.

Da ciò ne consegue l'obbligo di una gestione aziendale "responsabile" che tenga conto dei rischi connessi all'attività svolta e che sia idonea a garantire la piena conformità del trattamento dei dati personali ai principi sanciti dal Regolamento e dalla legislazione nazionale e la responsabilizzazione del titolare del trattamento a cui viene affidato sia il compito di decidere autonomamente le modalità, le garanzie ed i limiti del trattamento dei dati personali in considerazione della realtà produttiva nella quale opera.

La PIA quindi deve valutare anche l'impegno progettuale, nell'ottica del principio di privacy by design, e l'azione concreta del titolare, nell'attuazione del concetto di privacy by default, rispetto l'organizzazione della gestione di tutti i trattamenti svolti.

Contenuti

La PIA deve contenere, oltre la generale e complessiva valutazione dell'impatto del trattamento sulle libertà e sui diritti delle persone fisiche, alcune parti ritenute inderogabilmente essenziali dal DGPR (art.35 c.7 GDPR):

1. DESCRIZIONE GENERALE DEL TRATTAMENTO COMPLESSIVO: contenente la descrizione sistematica del trattamento complessivo e delle singole procedure che lo compongono, delle finalità e, se possibile, l'esplicazione dell'interesse legittimo perseguito dal titolare (art.35 c.7 p.a GDPR)[28].
2. VALUTAZIONE DELLA PROPORZIONALITÀ: di tutti i singoli trattamenti valutati in relazione alle loro finalità (art.35 c.7 p.b GDPR)[29].
3. RISK ANALYSIS: ossia una valutazione dettagliata dei rischi derivanti dal trattamento che possano sui diritti e sulle libertà degli interessati (art.35 c.7 p.c GDPR)[30].
4. IL PROGETTO OPERATIVO: contenente il dettaglio delle misure di sicurezza predisposte per affrontare i rischi sulla sicurezza dei dati personali nella misura più efficace in modo da poter dimostrare la conformità del trattamento alle precisioni del Regolamento Europeo (art.35 c.7 p.d GDPR)[31].

---

[28] Reg.UE/2016/679 GDPR, art.35 c.7 p.a "La valutazione contiene almeno: a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento; …".

[29] Reg.UE/2016/679 GDPR, art.35 c.7 p.b "La valutazione contiene almeno: …b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità; …".

[30] Reg.UE/2016/679 GDPR, art.35 c.7 p.c "La valutazione contiene almeno: … c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1 [ndr art.35 c.1: «Quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche,…»]; …".

[31] Reg.UE/2016/679 GDPR, art.35 c.7 p.c "La valutazione contiene almeno: … d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.".

Esiti finali della PIA

Acclarato che l'obiettivo sostanziale della PIA è quello di rendere più vicino possibile allo zero il rischio di procurare danni alle libertà e ai diritti o all'interessato, essa compie una valutazione puntuale dello stato di fatto ("as is") ponendo la sua attenzione sui rischi legati al trattamento e valutandoli al netto delle attività poste in essere o pianificate per contenerlo e ridimensionarlo sulla base delle valutazioni del titolare del trattamento e del il suo Staff (DPO, privacy manager, privacy specialist).

All'esito dello svolgimento della valutazione d'impatto si possono avere differenti conseguenze:

1. ELIMINAZIONE O COMPENSAZIONE DEI RISCHI.

Qualora il titolare riesca con il processo di PIA a identificare correttamente e a eliminare o attenuare sufficientemente il rischio, inizia il trattamento dopo aver completato la valutazione d'impatto, con il percorso previsto dal GDPR, rendendo disponibile la PIA agli organi di controllo e a chi ne abbia titolo.

2. SUSSISTENZA RESIDUA DI RISCHI.

Quando all'esito della valutazione d'impatto si ritenga che il trattamento mantenga rischi elevati residuali, il trattamento non può aver luogo e si deve procedere alla preventiva consultazione del Garante[32], in questo caso il titolare del trattamento deve inviare la PIA[33] all'Autorità di controllo e deve comunicare:

1. LE FINALITÀ E I MEZZI DEL TRATTAMENTO (art.36 c.3 p.b GDPR)[34];
2. I RUOLI DEPUTATI AL TRATTAMENTO: dettagliando le responsabilità del titolare del trattamento, l'eventuale presenza e l'accordo sulla ripartizione del trattamento con contitolari del trattamento, la nomina di responsabili del trattamento, il tutto con particolare attenzione nel caso in cui il trattamento avvenga nell'ambito di un gruppo imprenditoriale (art.36 c.3 p.a GDPR)[35];
3. LE MISURE DI SICUREZZA: che sono state previste per proteggere i diritti e le libertà degli interessati e per rendere quindi il trattamento conforme al regolamento (art.36 c.3 p.c GDPR)[36];

---

[32] Reg.UE/2016/679 GDPR, articolo 36 (Consultazione preventiva): "1.Il titolare del trattamento, prima di procedere al trattamento, consulta l'autorità di controllo qualora la valutazione d'impatto sulla protezione dei dati a norma dell'articolo 35 indichi che il trattamento presenterebbe un rischio elevato in assenza di misure adottate dal titolare del trattamento per attenuare il rischio.".

[33] Reg.UE/2016/679 GDPR, art.36 c.3 p.e: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: e) la valutazione d'impatto sulla protezione dei dati di cui all'articolo 35; …".

[34] Reg.UE/2016/679 GDPR, art.36 c.3 p.b: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: … b) le finalità e i mezzi del trattamento previsto; …".

[35] Reg.UE/2016/679 GDPR, art.36 c.3 p.a: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: a) ove applicabile, le rispettive responsabilità del titolare del trattamento, dei contitolari del trattamento e dei responsabili del trattamento, in particolare relativamente al trattamento nell'ambito di un gruppo imprenditoriale;…".

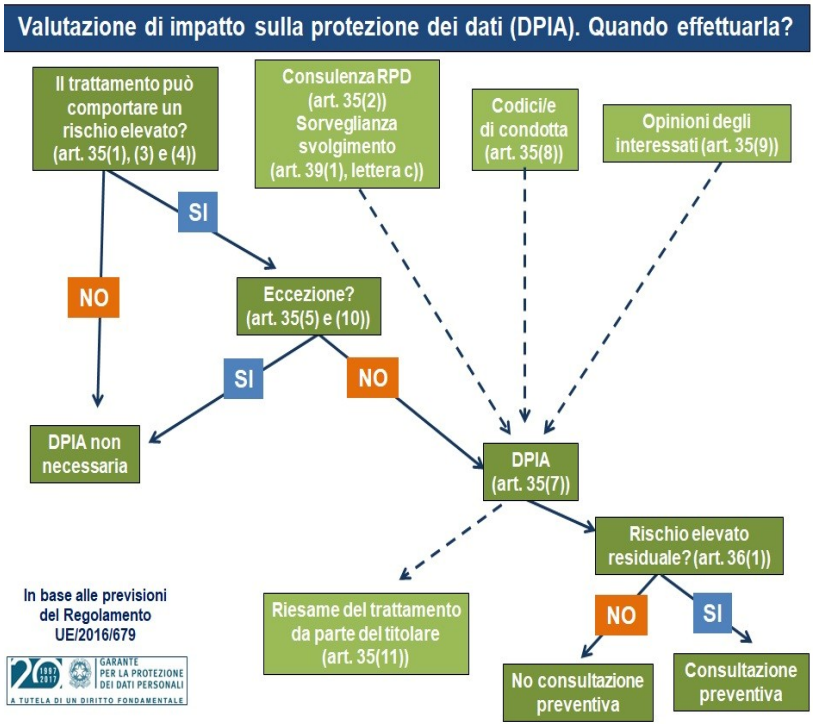
[36] Reg.UE/2016/679 GDPR, art.36 c.3 p.c: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: … c) le misure e le garanzie previste per proteggere i diritti e le libertà degli interessati a norma del presente regolamento; …".

4. I DATI E I RECAPITI DEL DPO (art.36 c.3 p.d GDPR)[37];
5. OGNI ALTRA INFORMAZIONE UTILE: che sia richiesta dall'autorità di controllo (art.36 c.3 p.f GDPR)[38].

Se il Garante ritenga che il trattamento violi il GDPR poiché il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce un parere scritto, entro otto settimane dalla richiesta di consultazione al titolare del trattamento e, se presente, al responsabile del trattamento, il termine può essere ulteriormente prorogato di sei settimane nei casi di trattamenti particolarmente complessi, previo avviso.[39]

Schemi grafici riepilogativi

Di seguito uno schema riepilogativo dell'obbligo di PIA preso dal sito del Garante per la Protezione dei Dati Personali.



[37] Reg.UE/2016/679 GDPR, art.36 c.3 p.d: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: … d) ove applicabile, i dati di contatto del responsabile della protezione dei dati;…".

[38] Reg.UE/2016/679 GDPR, art.36 c.3 p.f: "Al momento di consultare l'autorità di controllo ai sensi del paragrafo 1, il titolare del trattamento comunica all'autorità di controllo: … f) ogni altra informazione richiesta dall'autorità di controllo.".

[39] Reg.UE/2016/679 GDPR, art.36 c.2: "Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.".

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Scheda aggiornata in base alla versione delle Linee guida del WP29 emendata e adottata il 4 ottobre 2017

Valutazione di impatto sulla protezione dei dati (DPIA) – Art. 35 del Regolamento UE/2016/679

COSA È?

È una procedura prevista dall'**articolo 35 del Regolamento UE/2016/679 (RGDP)** che mira a descrivere un trattamento di dati per **valutarne la necessità e la proporzionalità nonché i relativi rischi**, allo scopo di approntare misure idonee ad affrontarli. Una DPIA **può riguardare un singolo trattamento oppure più trattamenti** che presentano **analogie** in termini di natura, ambito, contesto, finalità e rischi.

PERCHÉ?

La DPIA è uno strumento importante in termini di responsabilizzazione *(accountability)* in quanto aiuta il titolare non soltanto a rispettare le prescrizioni del RGPD, ma anche ad attestare di aver adottato misure idonee a garantire il rispetto di tali prescrizioni. In altri termini, **la DPIA è una procedura che permette di valutare e dimostrare la conformità con le norme in materia di protezione dei dati personali.** Vista la sua utilità, il Gruppo Art. 29 suggerisce di valutarne l'impiego **per tutti i trattamenti**, e **non solo** nei casi in cui il Regolamento la prescrive come obbligatoria.

IN CHE MOMENTO?

La DPIA deve essere condotta **prima** di procedere al trattamento. Dovrebbe comunque essere previsto un **riesame continuo** della DPIA, **ripetendo la valutazione a intervalli regolari.**

CHI?

La **responsabilità** della DPIA spetta al **titolare**, anche se la conduzione materiale della valutazione di impatto può essere affidata a un altro soggetto, interno o esterno all'organizzazione. Il titolare **ne monitora** lo svolgimento **consultandosi** con il **responsabile della protezione dei dati** (RPD, in inglese DPO) e acquisendo - se i trattamenti lo richiedono - il parere di esperti di settore, del **responsabile della sicurezza dei sistemi informativi** *(Chief Information Security Officer, CISO)* e **del responsabile IT.**

QUANDO LA DPIA E' OBBLIGATORIA?

In tutti i casi in cui un trattamento può presentare un **rischio elevato per i diritti e le libertà** delle persone fisiche.
Il Gruppo Art. 29 individua alcuni criteri specifici a questo proposito:
- trattamenti valutativi o di *scoring*, compresa la profilazione;
- decisioni automatizzate che producono significativi effetti giuridici (es: assunzioni, concessione di prestiti, stipula di assicurazioni);
- monitoraggio sistematico (es: videosorveglianza);
- trattamento di dati sensibili, giudiziari o di natura estremamente personale (es: informazioni sulle opinioni politiche);
- trattamenti di dati personali su larga scala;
- combinazione o raffronto di insiemi di dati derivanti da due o più trattamenti svolti per diverse finalità e/o da titolari distinti, secondo modalità che esulano dal consenso iniziale (come avviene, ad esempio, con i Big Data);
- dati relativi a soggetti vulnerabili (minori, soggetti con patologie psichiatriche, richiedenti asilo, anziani, ecc.);
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative (es: riconoscimento facciale, device IoT, ecc.);
- trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto (es: screening dei clienti di una banca attraverso i dati registrati in una centrale rischi per stabilire la concessione di un finanziamento).

La DPIA è necessaria in presenza di almeno due di questi criteri, ma - tenendo conto delle circostanze - il titolare può decidere di condurre una DPIA anche se ricorre uno solo dei criteri di cui sopra.

QUANDO LA DPIA NON E' OBBLIGATORIA?

Secondo le Linee guida del Gruppo Art. 29, la DPIA **NON è necessaria** per i trattamenti che:
- non presentano rischio elevato per diritti e libertà delle persone fisiche;
- hanno natura, ambito, contesto e finalità molto simili a quelli di un trattamento per cui è già stata condotta una DPIA;
- sono stati già sottoposti a verifica da parte di un'Autorità di controllo prima del maggio 2018 e le cui condizioni (es: oggetto, finalità, ecc.) non hanno subito modifiche;
- sono compresi nell'elenco facoltativo dei trattamenti per i quali non è necessario procedere alla DPIA;
- fanno riferimento a norme e regolamenti, Ue o di uno stato membro, per la cui definizione è stata condotta una DPIA.

La scheda ha un mero valore illustrativo ed è in continuo aggiornamento in base all'evoluzione delle indicazioni applicative del Regolamento. Per un quadro completo: www.garanteprivacy.it/regolamentoue

PARTE III-METODOLOGIA DI ESECUZIONE DELLA DPIA

Premessa metodologica

Il PIA (Privacy Impact Assessment) è un processo codificato e strutturato in fasi, dunque uno strumento operativo, che aiuta le organizzazioni aziendali ad analizzare con sistematicità, ad individuare e a ridurre i rischi privacy per gli individui interessati coinvolti dal rilascio di un nuovo progetto, soluzione o regola.

La valutazione d'impatto del trattamento dei dati personali costituisce parte integrante dell'approccio Privacy by Design, ed aiuta ad assicurare che i problemi potenziali siano identificati negli stadi iniziali del progetto quando la possibilità di indirizzarli è spesso più efficace e meno costosa.

Le sue fasi devono avere un ciclo ricorsivo per attualizzare la valutazione fatta inizialmente, a mano a mano che si procede con il progetto e vengono attuate le misure pianificate.

Le fasi del processo PIA possono essere condotte e registrate secondo il seguente schema:

1. VALUTAZIONE PRELIMINARE DI OPPORTUNITÀ PER UN PIA.

Questa fase serve a:

- spiegare ciò che il progetto intende realizzare,
- quali sono i benefici attesi per l'organizzazione,
- per gli individui e per le altre parti decidere, in base ad un insieme di domande mirate di screening, se un PIA sia necessario per dimensionare le risorse a seconda dell'entità del progetto e il tempo necessario alla valutazione capire gli impatti potenziali e i passi che potrebbero essere richiesti per identificare e ridurre il rischio.

2. DESCRIZIONE DEI FLUSSI DI INFORMAZIONI E COINVOLGIMENTO DEI PARTECIPANTI.

In questa fase si esegue una valutazione approfondita dei rischi e dei relativi impatti per la privacy e occorre valutare approfonditamente gli elementi che caratterizzano il trattamento dei dati descrivendo:

- quali informazioni sono utilizzate;
- come vengono trattate nelle singole fasi; cosa servono, ovvero per quale finalità; da chi sono ottenute, a chi sono comunicate; chi ne deve avere accesso.

In questa fase il processo di definizione della PIA può essere supportata da fonti informative già disponibili all'interno dell'organizzazione per descrivere come i dati saranno utilizzati, ad es. un diagramma che riporti i flussi informativi tra i vari soggetti o sistemi, la sequenza prevista delle operazioni di gestione dei dati, rapporti di audit sull'uso delle informazioni, mappe informative, registri di asset informativi.

Il DPO svolge un ruolo chiave con l'autorità di rivolgersi a chi è in grado di guidare le fasi del PIA sui processi esistenti ed inoltre può mantenere traccia di tutti i PIA eseguiti e di seguire le implicazioni derivanti dalla nuove procedure.

3. IDENTIFICAZIONE DEI RISCHI PRIVACY E DI QUELLI CORRELATI.

In questa fase occorre valutare gli aspetti di Privacy che espongono il progetto in esame a rischi di mancata tutela della Privacy: si deve tener presente che il processo PIA è insieme una forma di risk assessment e di risk management per quanto riguarda le implicazioni specifiche di Privacy.

Dunque l'organizzazione deve considerare come il progetto specifico potrà generare eventuali problemi alla privacy degli interessati che, a loro volta, si ripercuoteranno sulla stessa organizzazione se non indirizzati correttamente; ad esempio un progetto che è intrusivo sul fronte del pubblico aumenta anche i rischi di multe, di danni reputazionali, o di perdite di operatività se rilasciato con carenze o soluzioni inappropriate.

Si deve procedere a identificare e gestire in modo sistematico l'insieme dei rischi, basandosi soprattutto su quanto svolto nella fase precedente di descrizione dei flussi informativi raggruppandoli in stadi di utilizzo dei dati come una sequenza logica dei trattamenti, da quando i dati vengono ricevuti dall'esterno a quando vengono aggregati, elaborati, storicizzati e poi ulteriormente trasferiti.

È importante applicare a questi stadi un set di quesiti che consenta di far emergere le vulnerabilità e le minacce e su queste determinare gli effetti su cui quantificare gli impatti.

Laddove esistenti si possono utilizzare standard di settore o propri e metodologie di Project Management o di Risk Management per aiutarsi a categorizzare, identificare e misurare i rischi.

Il rischio deve essere valutato in termini di coefficienti di probabilità e di gravità secondo scale numeriche associate a classi di valori.

4. INDIVIDUAZIONE DELLE SOLUZIONI E DELLE MISURE.

In questa fase le organizzazioni hanno bisogno di identificare quali soluzioni possono essere intraprese per i rischi che hanno identificato.

Il PIA può offrire una serie di possibili opzioni per indirizzare ciascun rischio anche se va considerato che lo scopo non è quello di eliminare completamente l'impatto ma è quello di ridurre l'impatto ad un livello accettabile pur consentendo di realizzare un'iniziativa.

Dunque in questa fase, mentre si decide sulle possibili soluzioni, è sempre utile soppesare se gli scopi e i risultati del progetto sono proporzionati con l'impatto previsto sugli interessati e pertanto è opportuno tener traccia della misura di riduzione di rischio che ogni soluzione intende apportare.

Le organizzazioni hanno anche bisogno di valutare i costi e i benefici delle possibili soluzioni.

Alcuni costi sono di natura prettamente finanziari, ad esempio quando deve essere acquistato un nuovo software per garantire un maggiore controllo sull'accesso e sulla conservazione, ma i maggiori costi devono essere bilanciati rispetto ai benefici attesi, come per esempio una maggiore garanzia per proteggersi da violazioni dei dati, un minore rischio di sanzioni o provvedimenti o di essere esposti ad effetti reputazionali.

5. APPROVAZIONE DELLE DECISIONI E REGISTRAZIONE DEI RISULTATI.

Per le soluzioni che si è deciso di portare avanti è opportuno tener traccia dei passi seguiti nel processo decisionale, compreso chi li abbia approvati.

Nei casi in cui si fosse deciso di accettare un rischio, dovrebbe essere esplicita l'argomentazione sostenuta e l'assunzione di responsabilità.

Si ritiene utile giungere alla conclusione delle attività producendo un report finale, da allegare alla documentazione di progetto, per riassumere il processo e i passi compiuti per mitigare il

rischio privacy e per consentire di ricostruire a posteriori i motivi delle scelte fatte sulla base dei rischi individuati.

Si consideri che una registrazione del processo PIA può anche costituire una forma di comunicazione e di trasparenza verso gli interessati che ne richiedano la consultazione e diventare così una strategia di comunicazione, anche se il report PIA potrebbe non essere il solo documento prodotto come risultato del processo ma il PIA potrebbe aver fatto emergere il bisogno di una nuova comunicazione o regola da trasmettere agli interessati.

6. INTEGRAZIONE DEI RISULTATI DEL PIA NEL PIANO DI PROGETTO.

I rilievi PIA e le azioni in esso previste dovrebbero essere integrate con il piano di progetto complessivo man mano che si sviluppa.

Anche se la maggior parte dell'impegno per il PIA risiede nelle fasi iniziali del progetto, potrebbe essere necessario ritornare al PIA in vari stadi dello sviluppo e della realizzazione del progetto per avere conferma che le soluzioni sono state correttamente realizzate e hanno ottenuto l'effetto desiderato.

È probabile che i progetti di grande estensione ottengano benefici da un processo di revisione più formale.

Un PIA potrebbe generare azioni che continuano dopo che la valutazione è finita per cui è necessario che queste azioni vengano monitorate.

Sistema utilizzato per le mappature

Per la redazione delle sole mappe del rischio contenute nella presente PIA è stato utilizzato il software di ausilio ai titolari in vista della effettuazione della valutazione d'impatto sulla protezione dei dati messo a disposizione dal CNIL, l'Autorità francese per la protezione dei dati, sul sito www.cnil.fr (https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil), che segue un percorso di valutazione conforme alle indicazioni fornite dal WP29 nelle Linee-guida sulla DPIA.

In questo caso si è utilizzato la versione in lingua italiana che è stata messa a punto anche con la collaborazione del Garante per la protezione dei dati personali.

PARTE IV-VALUTAZIONE DEL CONTESTO

Mappaggio dei rischi

1.PIANO D'AZIONE

Principi fondamentali: Nessun piano d'azione registrato.

Misure esistenti o pianificate: Nessun piano d'azione registrato.

Rischi: Nessun piano d'azione registrato.

2.DPO AND DATA SUBJECTS OPINION

DPO/RPD: Ing. Antonio Lubrano Lavadera Via San Gennaro Agnano 84 - 80078 Pozzuoli(NA) Tel. 3389818689 – 3519680989 - Email antonio.lubranolavadera@tin.it pec: antonio.lubranolavadera@ingpec.eu

Parere del DPO/RPD
Allo stato attuale dei sistemi tecnologici e con le informazioni attualmente disponibili sul territorio interessato il trattamento si ritiene accettabile e implementabile.

3.RICHIESTA DEL PARERE DEGLI INTERESSATI

Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati: Il fondamento giuridico del trattamento dei dati risiede nell'assolvimento di funzioni ed obblighi di legge.

Contesto-Panoramica del trattamento

1.QUALE È IL TRATTAMENTO IN CONSIDERAZIONE? Sistema di videosorveglianza del Comune di Venticano. Esso svolge funzioni di prevenzione e rilevamento di reati e illeciti amministrativi oltre che a verificare i flussi di traffico.

2.QUALI SONO LE RESPONSABILITÀ CONNESSE AL TRATTAMENTO?

Titolare del trattamento dei dati personali è il Sindaco p.t. nella persona attualmente del dott. Luigi De Nisco.

Responsabili e/o Incaricati del trattamento dei dati, secondo le scelte del titolare del trattamento dei dati, sono le n. 02 unità in servizio presso l'Ufficio di Polizia Locale.

3.CI SONO STANDARD APPLICABILI AL TRATTAMENTO?

Ai fini del rilevamento di illeciti penali si deroga dalla normativa in materia di protezione dei dati personali in quanto la materia di polizia giudiziaria è esclusa, come tutte le attività giurisdizionali, dal campo di applicazione del Reg. UE 2016/679 GDPR.

Per le altre attività si utilizzeranno le privacy polities indicate nel Registro del Trattamento, in particolare si applicheranno le linee guida del EDPB e del Garante Italiano della Privacy.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Contesto-Dati, processi e risorse di supporto

1.QUALI SONO I DATI TRATTATI?

Riprese audiovisive di veicoli e cittadini che transitano sulle aree pubbliche del territorio comunale di Venticano, inclusi volti e numeri di targa che sono sottoposti a elaborazione OCR.

2.QUAL È IL CICLO DI VITA DEL TRATTAMENTO DEI DATI (DESCRIZIONE FUNZIONALE)?

Il dato viene rilevato dalle telecamere e mostrato in tempo reale agli operatori preposti, quindi viene immagazzinato in un sistema DVR, protetto dagli accessi fisici e informatici, quindi cancellato automaticamente, dopo il termine fissato dal Titolare del trattamento e indicato nei paragrafi successici.

3.QUALI SONO LE RISORSE DI SUPPORTO AI DATI?

I dati sono gestiti mediante applicativi proprietari installati su PC con sistemi operativi Windows con protezione antivirus/antimalaware e sistema di controllo accessi.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Principi Fondamentali-Proporzionalità e necessità

1.GLI SCOPI DEL TRATTAMENTO SONO SPECIFICI, ESPLICITI E LEGITTIMI?

Le finalità del trattamento sono specificatamente: la vigilanza sulla sicurezza urbana e quindi la prevenzione e l'eventuale accertamento di violazioni in materia penale ed amministrativa.

Il sistema è impiegato anche per il controllo del traffico cittadino al fine di prevenire ingorghi e intralci alla circolazione stradale.

Inoltre, il posizionamento di alcune telecamere anche in zone rurali e agricole svolge la funzione di prevenzione e rilevamento di incendi boschivi e scarichi abusivi.

Tali attività sono esplicitate attraverso idonea cartellonistica indicativa dell'attività di videosorveglianza posta nelle aree sottoposte a controllo e, specificatamente, in corrispondenza delle telecamere con pannelli ben visibili a distanza.

Le finalità rientrano nei compiti e nelle funzioni attribuite all'ente comunale ed alla Polizia Municipale di Venticano.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

2.QUALI SONO LE BASI LEGALI CHE RENDONO LECITO IL TRATTAMENTO?

Il trattamento si basa sulle competenze attribuite dalla legge all'ente e, tra le altre, in particolare dal d.lgs.267/2000 "Testo Unico degli Enti Locali", dalla legge 65/1986 "Legge quadro sull'ordinamento della Polizia Municipale" e dal d.lgs.1/2018 "Codice della Protezione Civile".

Valutazione : *Accettabile.*
Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

3.I DATI RACCOLTI SONO ADEGUATI, PERTINENTI E LIMITATI A QUANTO È NECESSARIO IN RELAZIONE ALLE FINALITÀ PER CUI SONO TRATTATI (MINIMIZZAZIONE DEI DATI)?

Vengono rilevate e registrate le immagini di specifiche porzioni di territorio che siano attinenti e conformi alle finalità del trattamento, come ad es.particolari tratti stradali, zone ove avvengono frequenti violazioni alle norme, parti del territorio dove si ritiene possano avvenire deposito di materiali di scarto o più in generali rifiuti civili e/o industriali, o anche parti di territorio boschivo nel quale si ritiene più elevato il rischio di incendio (in questo caso la distanza e l'estensione dell'area non rileva oggettivamente dati personali apprezzabili).

Inoltre le immagini vengono conservate per un periodo limitato e quindi eliminate automaticamente in maniera sicura sovrascrivendo i nuovi dati su quelli vecchi.

Valutazione : *Accettabile.*
Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

4.I DATI SONO ESATTI E AGGIORNATI?

Al fine della verifica della correttezza e dell'aggiornamento dei dati si stabilisce la prima verifica entro sei mesi dalla redazione del presente documento.

Valutazione : *Accettabile.*
Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

5.QUAL È IL PERIODO DI CONSERVAZIONE DEI DATI?

Le immagini registrate possono essere conservate sino a 18 mesi, in conformità alle vigenti norme in materia[40], con cancellazione automatica e sicura dei dati mediante sovrascrittura, salvo estrazione e

[40] 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. Decreto del Presidente della Repubblica 15 gennaio 2018, n. 15. da organi, uffici e comandi di polizia. Art.10. *Termini di conservazione dei dati* c.3 "u) dati raccolti mediante sistemi di ripresa fotografica audio e video nei servizi di ordine pubblico e di polizia giudiziaria - 3 anni dalla raccolta; dati raccolti mediante sistemi di videosorveglianza o di ripresa fotografica audio e video di documentazione dell'attività operativa - 18 mesi dalla raccolta. Si applicano i diversi termini di conservazione di cui alla lettera b) quando i dati personali sono confluiti in un procedimento per l'applicazione di una misura di prevenzione o quelli di cui alle lettere a) f) g) h) e i) quando i dati personali sono confluiti in un procedimento penale.".

conservazione di porzioni di registrazioni costituenti prova del procedimento penale e/o amministrativo e nei limiti tassativi di quanto necessario.

Il titolare del trattamento dei dati in accordo con le esigenze rappresentate dal comandante della Polizia Municipale fisserà la durata nel dettaglio.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

PARTE V - MISURE A TUTELA DEGLI INTERESSATI

1.COME SONO INFORMATI DEL TRATTAMENTO GLI INTERESSATI?

Le postazioni di ripresa ove sono installate le telecamere sono opportunamente evidenziate mediante cartellonistica contenente vignetta informativa conforme alle indicazioni di cui punto 7.1.2 n.114 delle Linee Guida 3/2019 pag.28[41] e punto 38 WP260[42] in quanto essa contiene:

- la finalità del trattamento;
- l'identità del titolare del trattamento ossia Comune di Venticano nella persona del Sindaco p.t.;
- l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento;
- i legittimi interessi perseguiti dal titolare;
- i recapiti del responsabile della protezione dei dati-DPO.

---

[41] European Data Protection Board Linee Guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video. Punto 7.1.2 Contenuto delle informazioni di primo livello "114. Generalmente, le informazioni di primo livello (segnale di avvertimento) dovrebbero comunicare i dati più importanti, ad esempio le finalità del trattamento, l'identità del titolare del trattamento e l'esistenza dei diritti dell'interessato, unitamente alle informazioni sugli impatti più consistenti del trattamento. Si può fare riferimento, ad esempio, ai legittimi interessi perseguiti dal titolare (o da un soggetto terzo) e ai recapiti del responsabile della protezione dei dati (se applicabile). Occorre anche fare riferimento alle informazioni di secondo livello, più dettagliate indicando dove e come trovarle."

[42] Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) [Linee guida elaborate dal Gruppo Art. 29 in materia di trasparenza (WP 260), definite in base alle previsioni del Regolamento (UE) 2016/679 Versione adottata l'11 aprile 2018]. Punto 38 "A layered approach to the provision of transparency information to data subjects can also be deployed in an offline/ non-digital context (i.e. a real-world environment such as person-toperson engagement or telephone communications) where multiple modalities may be deployed by data controllers to facilitate the provision of information. (See also paragraphs 33 to 37 and 39 to 40 in relation to different modalities for providing the information.) This approach should not be confused with the separate issue of layered privacy statements/ notices. Whatever the formats that are used in this layered approach, WP29 recommends that the first "layer" (in other words the primary way in which the controller first engages with the data subject) should generally convey the most important information (as referred to at paragraph 36 above), namely the details of the purposes of processing, the identity of controller and the existence of the rights of the data subject, together with information on the greatest impact of processing or processing which could surprise the data subject. For example, where the first point of contact with a data subject is by telephone, this information could be provided during the telephone call with the data subject and they could be provided with the balance of the information required under Article 13/ 14 by way of further, different means, such as by sending a copy of the privacy policy by email and/ or sending the data subject a link to the controller's layered online privacy statement/ notice.".

Essa è ben visibile a distanza che segnala l'area sottoposta a videosorveglianza indicando anche il titolare del trattamento dei dati, fornendo una informativa sintetica dei dati e delle informazioni obbligatorie per legge e rinviano al sito istituzionale del Comune per l'informativa completa.

Tutti gli interessati possono prendere visione e stampare copia dell'informativa completa sul trattamento dei dati personali dal sito del Comune di Venticano ovvero ottenerne copia fisica accedendo agli uffici comunali.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

2.OVE APPLICABILE: COME SI OTTIENE IL CONSENSO DEGLI INTERESSATI?

Il consenso degli interessati non è richiesto in quanto il fondamento giuridico del trattamento risiede nell'assolvimento di obblighi di vigilanza sulla sicurezza in ambito urbano (security & safety), di prevenzione ed accertamento dei reati e delle violazioni amministrative previsti dalla legge e rimessi alla competenza, in via principale o concorrente, dell'ente comunale e della Polizia Locale.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

3.COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI ACCESSO E DI PORTABILITÀ DEI DATI?

Con le stesse modalità previste per ottenere l'informativa completa sul trattamento dei dati personali, è possibile esercitare i diritti degli interessati previsti dalle norme, mediante richiesta rivolta al Titolare del trattamento dei dati personali in forma elettronica, via mail e pec, o cartacea, attraverso raccomandata o nota depositata al protocollo del Comune.

Nelle informative sintetiche, poste in corrispondenza e nelle aree sottoposte a videosorveglianza è indicata la normativa che regola la materia e, comunque, sul sito del Comune di Venticano è visionabile l'informativa completa.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

4.COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI RETTIFICA E DI CANCELLAZIONE (DIRITTO ALL'OBLIO)?

Il diritto all'oblio si realizza automaticamente entro i termini di cancellazione delle immagini registrate che avviene automaticamente.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

5.COME FANNO GLI INTERESSATI A ESERCITARE I LORO DIRITTI DI LIMITAZIONE E DI OPPOSIZIONE?

Rivolgendo istanza al titolare e/o al responsabile del trattamento ovvero al RPD/DPO, i cui riferimenti, così come le modalità per contattarli, sono indicate nell'informativa completa sul sito del comune *www.comune.venticano.av.it*.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

6.GLI OBBLIGHI DEI RESPONSABILI DEL TRATTAMENTO SONO DEFINITI CON CHIAREZZA E DISCIPLINATI DA UN CONTRATTO?

Sono contenute nell'atto di incarico e nel Regolamento della Videosorveglianza e privacy policies. Il contratto non è previsto in quanto la persona designata è già legato da un rapporto contrattuale con l'Ente e pertanto la nomina e le indicazioni derivano da atto autoritativo di diritto amministrativo.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

7.IN CASO DI TRASFERIMENTO DI DATI AL DI FUORI DELL'UNIONE EUROPEA, I DATI GODONO DI UNA PROTEZIONE EQUIVALENTE?

Non è previsto alcun trasferimento al di fuori dell'Unione Europea.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

PARTE VI - VALUTAZIONE DEL SISTEMA

Breve descrizione tecnica dell'impianto

Trattasi di un impianto che complessivamente si compone di n. 72 telecamere distribuite sul territorio comunale con una attenta scelta della loro ubicazione sia per gli aspetti propri della governance del territorio che di quelli propri della robustezza dell'impianto:

- Sono state istallate due tipi di telecamere e precisamente di "contesto" ed "ocr";
- Tutte le telecamere sono dotate di un sistema ridondante di alimentazione, batterie ricaricate autonomamente mediante energia elettrica addizionale; quando ci si è trovati nella indisponibilità di un collegamento elettrico, per esempio derivandolo dall'impianto di illuminazione pubblica, si sono istallati pannelli fotovoltaici a supporto in alternativa.
- Tutte le telecamere sono dotate di autonomia di registrazione e utilizzano la loro memoria interna in caso di indisponibilità delle linee di trasmissione dati. Queste ultime trasferiscono, in real time, il segnale video criptato al sistema centrale di visualizzazione e memorizzazione, situato nella cabina di regia tecnica presso il Comando dei Vigili Urbani.
- Laddove ci si è trovati nella necessità di istallare pali e telecamere prive di ogni supporto e possibilità di essere raggiunte agevolmente da linee dati (per quelle elettriche si è aggirato l'ostacolo utilizzando pannelli fotovoltaici), si è progettato e realizzato un sistema di ponti a radiofrequenza per coprire tali distanze.
- La cabina di regia dell'impianto è dotata di numerosi video partizionati a supporto delle riprese provenienti da tutte le telecamere. Inoltre si utilizza DVR per la registrazione dei segnali video. La memorizzazione normalmente sovrascrive le vecchie registrazione dopo **sette giorni**, in accordo con il regolamento della videosorveglianza del Comune di Venticano.

Rischi - Misure di sicurezza esistenti o pianificate

1.CRITTOGRAFIA

Le telecamere dispongono di sistema di registrazione criptato su memoria SIM locale e remota su DVR con connessione fisica o Via radiofrequenza tra sistemi di ripresa (telecamera IP) e di registrazione (server DVR).

Le telecamere sono installate su solidi pali posti a rilevante altezza dal suolo in modo da non poter essere agevolmente manomesse o asportate.

Le immagini fotografiche e audiovisive registrate sono criptate con sistema proprietario che permette di visionarle solo disponendo della chiave di crittografia.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

2.TRACCIABILITÀ

Le telecamere sono visualizzabili in tempo reale mediante lo stesso server di registrazione che è posto in luogo sicuro e presidiato e precisamente denominato "Cabina di Regia" nell'ufficio della Polizia Municipale. I dati registrati sono completati con il tag contenente le informazioni relative alla posizione della telecamera che li ha ripresi con l'aggiunta della loro cronodatazione.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

3.CONTROLLO DEGLI ACCESSI LOGICI

Il controllo degli accessi per la visualizzazione in tempo reale è consentito solo sul server del sistema e sul DVR ed è protetto da password. Possono accedervi solo il responsabile e/o l'incaricato al trattamento dati designato con specifico atto di nomina.

Il controllo dell'accesso ai dati registrati è realizzato mediante la crittografia dei dati che consente solo ai soggetti in possesso della chiave autorizzati di avere l'accesso alle immagini fotografiche e ai filmati audiovisivi, mediante la chiave di crittografia.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

Rischi-Accesso illegittimo ai dati

1.QUALI POTREBBERO ESSERE I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Qualora si concretizzasse un accesso abusivo al sistema da soggetti attrezzati e travisati (in quanto le telecamere sono installate a rilevante altezza su palo non accessibile da terra), e fosse infine possibile asportare la memoria di massa senza/nonostante il pronto intervento dei sistemi di sicurezza, ed infine si riuscisse a rendere in chiaro i dati crittografati, si avrebbe visione dei dati registrati. Questi ultimi sarebbero, quindi, quelli dei veicoli e delle persone che sono transitati nell'area di registrazione, con differente qualità delle immagini a secondo se trattasi di telecamera di contesto o di OCR. Comunque le informazioni presenti nelle telecamere e da essa temporaneamente depositate sulla SIM on board dovrebbero già essere state inviate e registrate sul DVR nella "Cabina di Regia". L'eventuale manomissione di una telecamera, quindi, in generale, non comporta la perdita dei dati e probabilmente saranno disponibili anche dati relativi al momento della manomissione.

Nella condizione peggiore, anche se si asportasse completamente la telecamera, le immagini registrate sul DVR potrebbero dare informazioni circa i soggetti e l'azione vandalica o criminale messa in atto e consentirebbe di rilevare anche la presenza di veicoli sospetti. Comunque tali dati tuttavia sarebbero rilevabili anche con l'osservazione legittima, poiché avvenuti su aree pubbliche: quindi, la perdita delle informazioni o prove e dell' individuabilità dei responsabili è piuttosto improbabile per la contestuale registrazione sul DVR della "Cabina di Regia".

2.QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONCRETIZZARE IL RISCHIO?

Furto o vandalismo al sistema di videosorveglianza e registrazione dei dati.

3.QUALI SONO LE FONTI DI RISCHIO?

Non stimabili al momento

4.QUALI MISURE FRA QUELLE INDIVIDUATE CONTRIBUISCONO A MITIGARE IL RISCHIO?

Crittografia, controllo degli accessi logici, ridondanza delle registrazioni.

5.COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Trascurabile, poiché il posizionamento delle telecamere su solidi pali posti a rilevante altezza dal suolo, la registrazione di dati criptati on board, la registrazione remota su DVR, il sistema di crittografia e il posizionamento del server di registrazione in un locale sicuro e presidiato qual è l'ufficio "Cabina di Regia" presso il servizio di Polizia Municipale rendono molto limitato se non trascurabile il rischio di accesso abusivo ai dati e limitato anche il rischio di distruzione degli stessi.

6.COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Trascurabile, le difficoltà oggettive e il rischio personale che si assumerebbe chi volesse asportare lo strumento di registrazione e di immagazzinamento dei dati sarebbe molto elevato (con conseguenze civili e penali gravi) rispetto il vantaggio conseguente, quindi la probabilità del rischio si può considerare trascurabile.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Rischi-Modifiche indesiderate dei dati

1.QUALI SAREBBERO I PRINCIPALI IMPATTI SUGLI INTERESSATI SE IL RISCHIO SI DOVESSE CONCRETIZZARE?

Perdita delle informazioni e quindi delle prove e dell'individuabilità dei responsabili, o, in alternativa, la visione dei soggetti e dei veicoli comunicherebbe la presenza degli stessi. Si precisa che tali dati possono essere stati rilevati anche con l'osservazione legittima, poiché avvengono su aree pubbliche.

In definitiva e con riferimento al caso in cui fosse realizzato un accesso abusivo al sistema da soggetti attrezzati e travisati (in quanto le telecamere sono installate a rilevante altezza su palo non accessibile da terra, e la Cabina di Regia è protetta all'interno della Casa Comunale), e fosse possibile asportare la memoria di massa senza il pronto intervento dei sistemi di sicurezza e si riuscisse a rendere in chiaro i dati crittografati, si avrebbe visione dei dati registrati quindi dei veicoli e delle persone che sono transitati nell'area di registrazione.

2.QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA CONCRETIZZAZIONE DEL RISCHIO?

Al momento non quantificabili.

3.QUALI SONO LE FONTI DI RISCHIO?

Non stimabili al momento.

4.QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Crittografia, controllo degli accessi logici, ridondanza dell'esplorazione e controllo delle aree urbane da parte di più telecamere.

5.COME STIMERESTE LA GRAVITÀ DEL RISCHIO, IN PARTICOLARE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Trascurabile, il sistema di crittografia e il controllo logico degli accessi rende pressoché impossibile l'accesso ai dati ai fini della modifica se non ai soggetti autorizzati e quindi formati e competenti.

6.COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO A MINACCE, FONTI DI RISCHIO E MISURE PIANIFICATE?

Trascurabile. In considerazione del controllo degli accessi logici, della crittografia dei dati e dei sistemi di sicurezza fisica e di allarme la probabilità del rischio è pressoché trascurabile.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Rischi-Perdita di dati

1.QUALI POTREBBERO ESSERE GLI IMPATTI PRINCIPALI SUGLI INTERESSATI SE IL RISCHIO DOVESSE CONCRETIZZARSI?

Perdita delle informazioni e quindi delle prove e dell'individuabilità dei responsabili.

2.QUALI SONO LE PRINCIPALI MINACCE CHE POTREBBERO CONSENTIRE LA MATERIALIZZAZIONE DEL RISCHIO?

Furto o vandalismo al sistema di videosorveglianza e registrazione dei dati, danno o malfunzionamento del sistema di registrazione dei dati.

3.QUALI SONO LE FONTI DI RISCHIO?

Non stimabili al momento.

4.QUALI MISURE, FRA QUELLE INDIVIDUATE, CONTRIBUISCONO A MITIGARE IL RISCHIO?

Controllo degli accessi logici.

5.COME STIMERESTE LA GRAVITÀ DEL RISCHIO, SPECIALMENTE ALLA LUCE DEGLI IMPATTI POTENZIALI E DELLE MISURE PIANIFICATE?

Trascurabile, la memoria di massa è affidabile rispetto i sistemi attualmente disponibili e la trasmissione dei dati da remoto permette di utilizzare un sistema affidabile e ridondante di registrazione.

6.COME STIMERESTE LA PROBABILITÀ DEL RISCHIO, SPECIALMENTE CON RIGUARDO ALLE MINACCE, ALLE FONTI DI RISCHIO E ALLE MISURE PIANIFICATE?

Trascurabile, il posizionamento della telecamera, i sistemi di sicurezza adottati rendono trascurabile il rischio, tuttavia potrebbe essere sostanzialmente eliminato con un sistema di ridondanza in RAID.

Valutazione : *Accettabile*.

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione*.

Rischi-Panoramica dei rischi

Impatti potenziali

Qualora fosse realizzato un
La visione dei soggetti e d..
Perdita delle informazioni .
Qualora fosse realizzato un

Minaccia

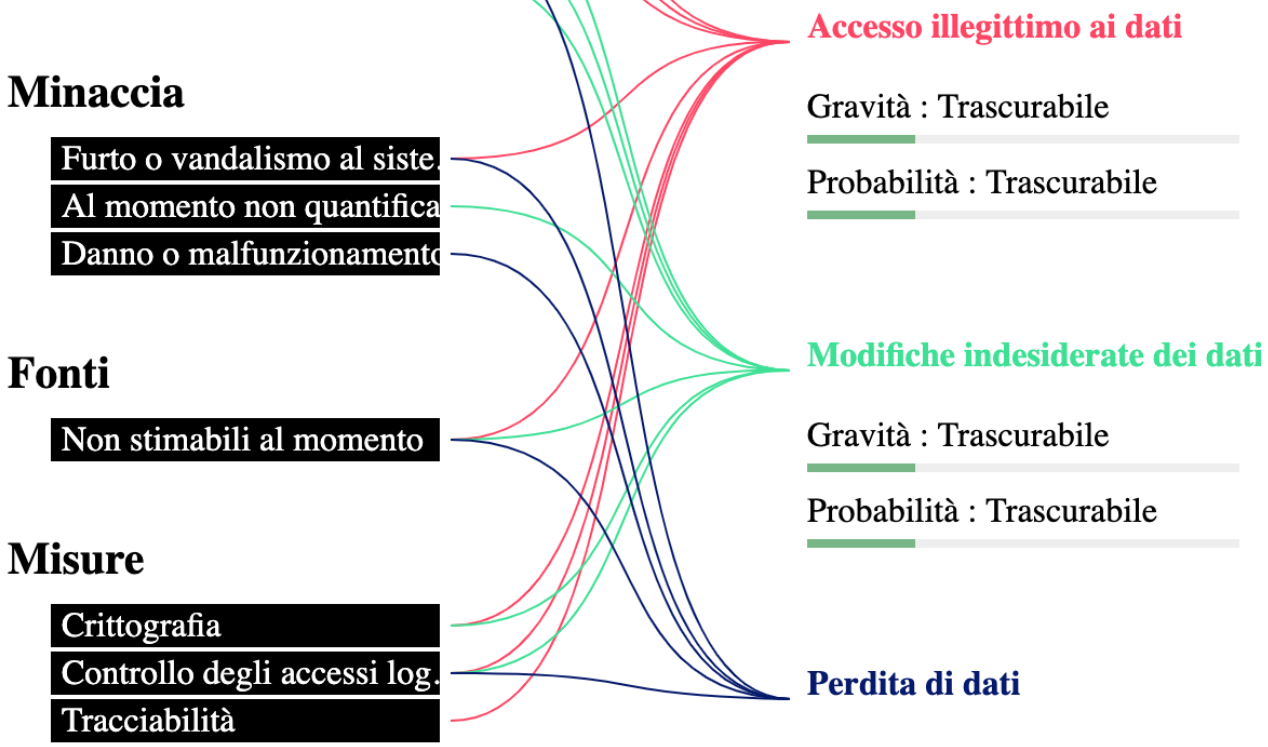
Furto o vandalismo al siste.
Al momento non quantifica
Danno o malfunzionamento

Fonti

Non stimabili al momento

Misure

Crittografia
Controllo degli accessi log.
Tracciabilità



Accesso illegittimo ai dati

Gravità : Trascurabile

Probabilità : Trascurabile

Modifiche indesiderate dei dati

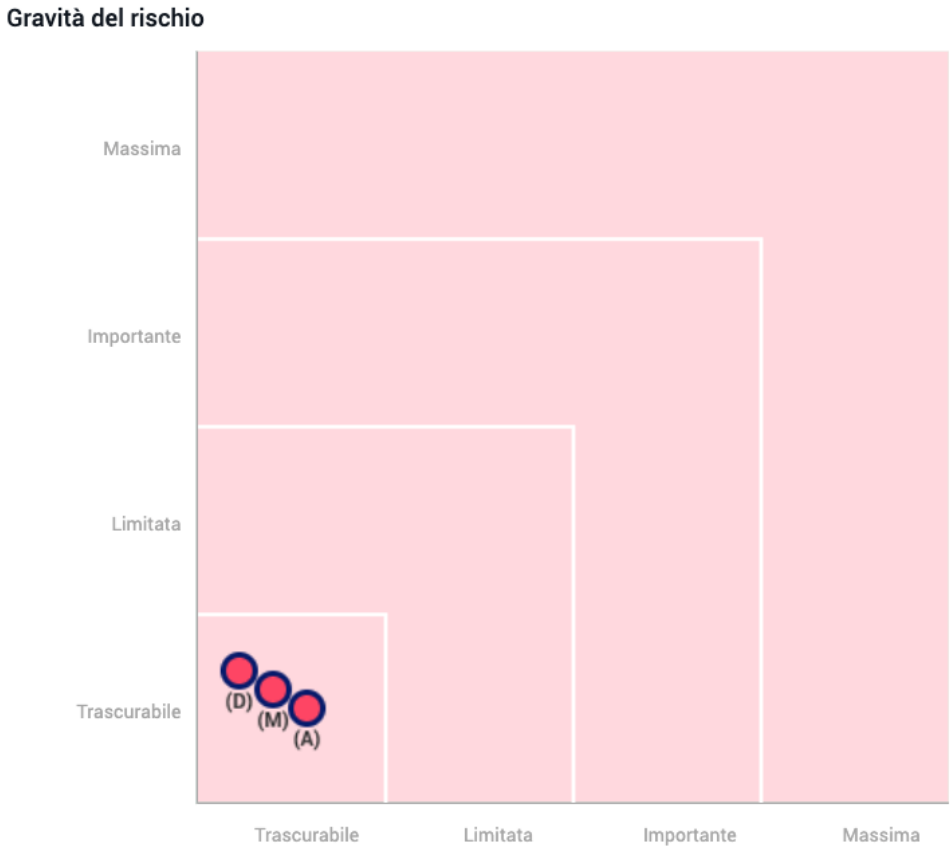
Gravità : Trascurabile

Probabilità : Trascurabile

Perdita di dati

Gravità : Trascurabile

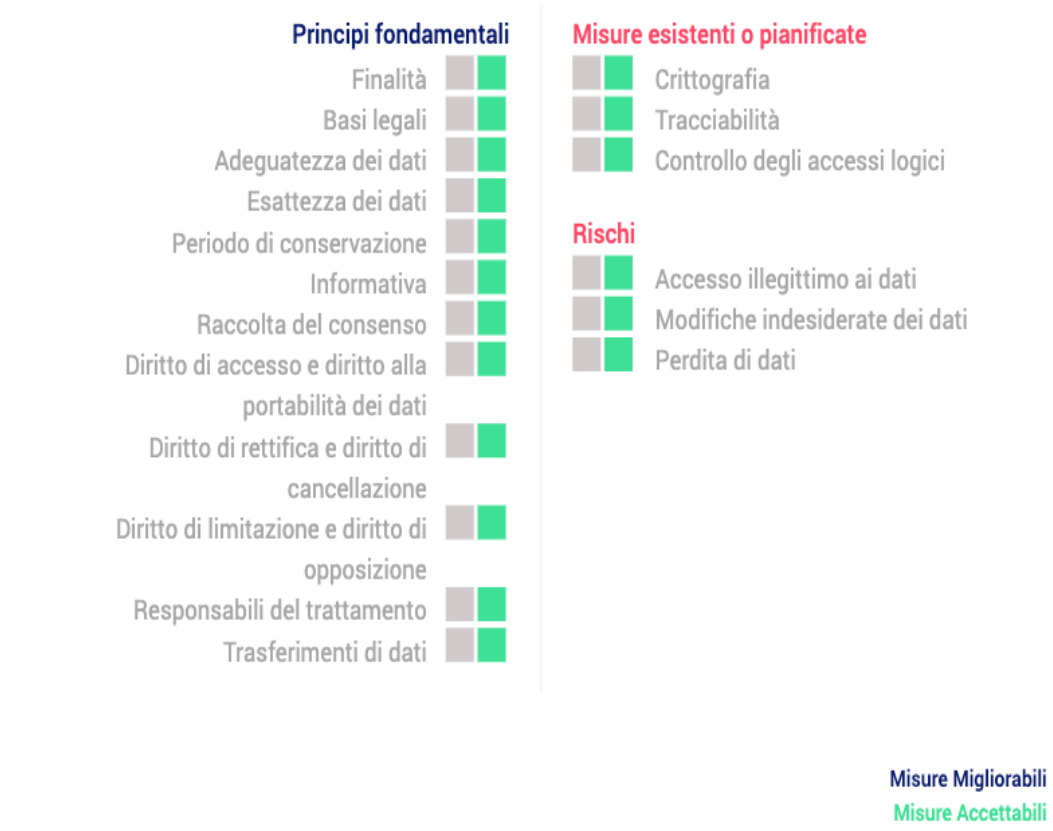
Probabilità : Trascurabile



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

20/07/2020

Panoramica


Principi fondamentali
Finalità
Basi legali
Adeguatezza dei dati
Esattezza dei dati
Periodo di conservazione
Informativa
Raccolta del consenso
Diritto di accesso e diritto alla portabilità dei dati
Diritto di rettifica e diritto di cancellazione
Diritto di limitazione e diritto di opposizione
Responsabili del trattamento
Trasferimenti di dati
Misure esistenti o pianificate
Crittografia
Tracciabilità
Controllo degli accessi logici
Rischi
Accesso illegittimo ai dati
Modifiche indesiderate dei dati
Perdita di dati
Misure Migliorabili
Misure Accettabili

PARTE VII-VALUTAZIONE DELLE SICUREZZE DEMOCRATICHE

Analisi del posizionamento delle telecamere sul territorio

1.PRINCIPI GENERALI

La videosorveglianza, comunque sia realizzata, dalle postazioni fisse a quelle mobili includendo anche quelle indossate dagli operatori, è consentita per la prevenzione e l'accertamento di illeciti a condizione che non comporti un'ingerenza ingiustificata nei diritti e nelle libertà fondamentali delle persone interessate[43].

La valutazione quindi deve avere inizio dal posizionamento delle telecamere per valutare i luoghi e i soggetti che possono essere ripresi e di conseguenza i dati personali che possono essere trattati per verificare, oltre il rispetto del principio generale di minimizzazione dei dati, la diretta correlazione con la funzione e l'attività di polizia (DPR 15/2018 art.3 c.1)[44].

2.VERIFICA POSIZIONAMENTO DELLE TELECAMERE

La planimetria allegata verificata in seguito a sopralluoghi svolti dal gruppo di progetto cui partecipa un componente dell'Ufficio Tecnico evidenzia il posizionamento delle telecamere del sistema di videosorveglianza del comune di Venticano.

Si può rilevare e si è accertato in via preliminare che esse non inquadrano:

- sedi di partiti e movimenti politici, che possano consentire di rilevare dati sulle frequentazioni e sulle preferenze politiche, anche in via presuntiva, dei soggetti ripresi;
- sedi di sindacati, che possano consentire di presumere appartenenze o simpatie sindacali;
- luoghi di culto, che permettano di rilevare le convinzioni religiose dei soggetti ripresi;
- scuole che siano seggi elettorali, che possano rilevare quali soggetti esercitino il diritto di voto e, in via induttiva e presuntiva, le idee politiche in funzione delle relazioni con eventuali candidati o rappresentanti di partiti e movimenti politici;

Sulla base dell'area di ripresa e dei sistemi di sicurezza adottati e illustrati in precedenza, allo stato non si ritiene che si possano dottare ulteriori misure per la minimizzazione dei dati e la sicurezza del trattamento dei dati.

---

[43] DPR 15/2018. 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.. Art. 3. *Finalità dei trattamenti* c.1 "I trattamenti di dati personali si intendono effettuati per le finalità di polizia, ai sensi dell'articolo 53 del Codice, quando sono direttamente correlati all'esercizio dei compiti di polizia di prevenzione dei reati, di tutela dell'ordine e della sicurezza pubblica, nonché di polizia giudiziaria, svolti, ai sensi del codice di procedura penale, per la prevenzione e repressione dei reati. …".

[44] Ibidem.

3.PLANIMETRIA POSIZIONAMENTO DELLE TELECAMERE

COMUNE DI VENTICANO

4.COME STIMARE LA PROBABILITÀ DEL RISCHIO CHE POSSANO ESSERE ACQUISITI DATI CHE POSSANO COMPROMETTERE I DIRITTI FONDAMENTALI DEI CITTADINI O CHE I DATI POSSANO ESSERE UTILIZZATI PER FINALITÀ ESTRANEI ALL'ATTIVITÀ DI POLIZIA?

Trascurabile, dato il posizionamento della telecamera, i sistemi di sicurezza adottati e i soggetti (polizia locale) che gestiscono e che hanno accesso ai dati.

Valutazione : *Accettabile.*

Commento di valutazione: *Il titolare del trattamento e il DPO considerano corretta la valutazione.*

PARTE VIII

INDICAZIONI DI SICUREZZA

Vigilanza, adeguamento e verifica

1.FORMAZIONE

L'obbligo di formazione previsto dalla vigente normativa (art.29 e 32 Reg.UE 2016/679 GDPR) che costituisce un dovere generale nell'ambito del principio di accountability, rende necessario e urgente non solo un percorso di retraining e aggiornamento per estendere a tutti i soggetti coinvolti, in ogni modo, la conoscenza e le cautele da adottare per la gestione dell'impianto di videosorveglianza e la corretta gestione del trattamento dei dati.

2.VERIFICA

La nuova installazione richiede la verifica dell'efficienza ed efficacia delle valutazioni eseguite in questa valutazione d'impatto e il riscontro all'atto del funzionamento operativo.

Allo scopo si suggerisce di prevedere:

- un primo sopralluogo e verifica ispettiva a 6 mesi dall'attivazione del sistema;
- Un ciclo di sopralluoghi e visite ispettive di verifica almeno annuali.

Venticano (AV), 10 Maggio 2021.

Il titolare del trattamento

IL Sindaco
F.to Dott. Luigi De Nisco

Il RDP/DPO

F.to Ing. Antonio Lubrano Lavadera