Regolamento comunale per l'attuazione del Regolamento UE 2016/679 disciplinante la protezione delle persone fisiche con riguardo al trattamento dei dati personali

INDICE

privacy (art.168 Dlgs 196/03)
Art.38 – Entrata in vigore
Art.39 - Rinvio

PREMESSA

A decorrere dal 25 maggio 2018 è entrato in vigore il nuovo regolamento UE, che si applica negli Stati membri ed ha ad oggetto la protezione delle persone fisiche, con riguardo al trattamento dei dati di carattere personale.

Per rafforzare la protezione, il Regolamento UE ha fondato il suo impianto su misure di accountability di titolari e responsabili (come la valutazione di impatto, il registro dei trattamenti, le misure di sicurezza, la nomina di un Responsabile Della Protezione-Data Protection Officer).
La nuova disciplina europea, quindi, pone l'accento sulla "responsabilizzazione" ossia, sull'adozione di comportamenti tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento. Tra i criteri che i titolari e i responsabili sono tenuti ad utilizzare nella gestione degli obblighi vi sono:
il criterio del "data protection by default and by design", ossia la necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili "al fine di soddisfare i requisiti" del regolamento e tutelare i diritti degli interessati tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati;

- il criterio del rischio inerente al trattamento, da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati, impatti che devono essere analizzati attraverso un apposito processo di valutazione tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il Titolare ritiene di dover adottare per mitigare tali rischi.

Il Comune di Salerno, Titolare del trattamento, nell'ottica di conformare la propria normativa alla nuova regolamentazione delle disposizioni in materia di protezione dei dati personali procede all'adozione del presente Regolamento.

Art. 1

Oggetto

1. Il presente Regolamento ha per oggetto misure procedimentali e regole di dettaglio ai fini della

migliore funzionalità ed efficacia dell'attuazione del Regolamento europeo (General Data Protection Regulation del 27 aprile 2016 n. 679, di seguito indicato con "RGPD", Regolamento Generale Protezione Dati), relativo alla protezione delle persone fisiche con riguardo ai trattamenti dei dati personali, nonché alla libera circolazione di tali dati, nel Comune di Salerno.

Art. 2

Finalità del trattamento

1. I trattamenti sono compiuti dal Comune per le seguenti finalità:

a) l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Rientrano in questo ambito i trattamenti compiuti per:

- l'esercizio delle funzioni amministrative che riguardano la popolazione ed il territorio, precipuamente nei settori organici dei servizi alla persona ed alla comunità, dell'assetto ed utilizzazione del territorio e dello sviluppo economico;

- la gestione dei servizi elettorali, di stato civile, di anagrafe, di leva militare e di statistica;

- l'esercizio di ulteriori funzioni amministrative per servizi di competenza statale affidate al Comune in base alla vigente legislazione.

La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

b) l'adempimento di un obbligo legale al quale è soggetto il Comune. La finalità del trattamento è stabilita dalla fonte normativa che lo disciplina;

c) l'esecuzione di un contratto con soggetti interessati;

d) per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

Art. 3

Definizioni

Ai fini del presente regolamento si adottano le seguenti definizioni:

Dati personali: qualunque informazione riguardante una persona fisica identificata o identificabile;

Dati relativi alla salute: dati personali sensibili sullo stato di salute fisica e mentale di una persona fisica, inclusa la prestazione di servizi di assistenza sanitaria, inclusi i dati genetici e biometrici;

Dati giudiziari: i dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza.

Titolare del trattamento: ente locale che anche congiuntamente determina e decide le finalità ed i mezzi del trattamento;

Responsabile del trattamento: persona fisica o giuridica o ente pubblico che tratta i dati per conto del Titolare del trattamento;

Destinatario: persona fisica o giuridica, ente pubblico che riceve comunicazione di dati personali;

Terzo: chiunque (persona fisica, giuridica, ente pubblico) diverso dall'interessato, dal titolare del trattamento, dal responsabile del trattamento, da ogni incaricato.

Trattamento : qualsiasi operazione compiuta con o senza processi automatizzati che prevede la raccolta, la registrazione, l'organizzazione, la strutturazione, conservazione, adattamento o modifica, l'estrazione, consultazione, utilizzo, trasmissione diffusione o altra forma di messa a disposizione di dati personali;

Consenso dell'interessato: ogni manifestazione di volontà libera, specifica, informata ed inequivocabile dell'interessato con cui viene manifestato il suo assenso e viene conferita legittimità al trattamento dei propri dati personali;

Profilazione: trattamento automatizzato di dati personali per valutare determinati aspetti personali relativi ad una persona fisica come a titolo esemplificativo, rendimento professionale, situazione economica;

Pseudonimizzazione: trattamento di dati in modo che non si possa risalire all'identificazione dell'interessato senza informazioni aggiuntive conservate separatamente e soggette a misure di sicurezza;

Violazione dei dati personali: ogni diffusione, trasmissione, accesso, comunicazione non autorizzata

Archivio: insieme strutturato di dati personali accessibili secondo criteri determinati;

Art. 4

Titolare del trattamento

1. Il Comune di Salerno , rappresentato ai fini previsti dal RGPD dal Sindaco pro tempore, è il Titolare del trattamento dei dati personali raccolti o meno in banche dati, automatizzate o cartacee (di seguito indicato con "Titolare"). Il Sindaco può delegare le relative funzioni a Dirigente/Responsabile P.O. in possesso di adeguate competenze.

2. Il Titolare è responsabile del rispetto dei principi applicabili al trattamento di dati personali stabiliti dall'art. 5 RGPD: liceità, correttezza e trasparenza; limitazione della finalità; minimizzazione dei dati; esattezza; limitazione della conservazione; integrità e riservatezza.

3. Il Titolare mette in atto misure tecniche ed organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento di dati personali è effettuato in modo conforme al RGPD.

Le misure sono definite fin dalla fase di progettazione e messe in atto per applicare in modo efficace i principi di protezione dei dati e per agevolare l'esercizio dei diritti dell'interessato stabiliti dagli articoli 15-22 RGPD, nonché le comunicazioni e le informazioni occorrenti per il loro esercizio.

Gli interventi necessari per l'attuazione delle misure sono considerati nell'ambito della programmazione operativa (DUP), di bilancio e di Peg, previa apposita analisi preventiva della situazione in essere, tenuto conto dei costi di attuazione, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi dallo stesso derivanti, aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche.

4. Il Titolare adotta misure appropriate per fornire all'interessato:

a) le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;

b) le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

5. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare deve effettuare una valutazione dell'impatto del trattamento sulla protezione dei dati personali (di seguito indicata con "DPIA") ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità del medesimo trattamento.

6. Il Titolare, inoltre, provvede a:

a) designare i Responsabili del trattamento nelle persone dei Dirigenti/Responsabili P.O. e dei Funzionari delle singole strutture in cui si articola l'organizzazione comunale, che sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza. Per il trattamento di dati il Titolare può avvalersi anche di soggetti pubblici o privati;

b) nominare il Responsabile della protezione dei dati;

c) nominare quale Responsabile del trattamento i soggetti pubblici o privati affidatari di attività e servizi per conto dell'Amministrazione comunale, relativamente alle banche dati gestite da soggetti esterni al Comune in virtù di convenzioni, di contratti, o di incarichi professionali o altri strumenti giuridici consentiti dalla legge, per la realizzazione di attività connesse alle attività istituzionali;

d) predisporre l'elenco dei Responsabili del trattamento delle strutture in cui si articola l'organizzazione dell'Ente, pubblicandolo in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. Nel caso di esercizio associato di funzioni e servizi, nonché per i compiti la cui gestione è affidata al Comune da enti ed organismi statali o regionali, allorché due o più titolari determinano congiuntamente, mediante accordo, le finalità ed i mezzi del trattamento, si realizza la contitolarità di cui

all'art. 26 RGPD. L'accordo definisce le responsabilità di ciascuno in merito all'osservanza degli obblighi in tema di privacy, con particolare riferimento all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni di cui agli artt. 13 e 14 del RGPD, fermo restando eventualmente quanto stabilito dalla normativa specificatamente applicabile; l'accordo può individuare un punto di contatto comune per gli interessati.

8. Il Comune favorisce l'adesione ai codici di condotta elaborati dalle associazioni e dagli organismi di categoria rappresentativi, ovvero a meccanismi di certificazione della protezione dei dati approvati, per contribuire alla corretta applicazione del RGPD e per dimostrarne il concreto rispetto da parte del Titolare e dei Responsabili del trattamento.

Art. 5

Responsabile del trattamento

1. Un Dirigente/Responsabile P.O. o più Dirigenti/Responsabili P.O. delle strutture di massima dimensione in cui si articola l'organizzazione dell'Ente, è nominato dal Titolare del trattamento con provvedimento motivato di Giunta o con provvedimento del Sindaco Responsabile del trattamento di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il Responsabile unico deve essere in grado di offrire garanzie sufficienti in termini di conoscenza specialistica, esperienza, capacità ed affidabilità, per mettere in atto le misure tecniche e organizzative di cui all'art. 6 rivolte a garantire che i trattamenti siano effettuati in conformità al RGPD.

2. I dipendenti del Comune, Responsabili del trattamento, sono designati, di norma, mediante decreto di incarico del Sindaco, nel quale sono tassativamente disciplinati:

- la materia trattata, la durata, la natura e la finalità del trattamento o dei trattamenti assegnati;

- il tipo di dati personali oggetto di trattamento e le categorie di interessati;

- gli obblighi ed i diritti del Titolare del trattamento.

Tale disciplina può essere contenuta anche in apposita convenzione o contratto da stipularsi fra il Titolare e ciascun responsabile designato.

3. Il Titolare può avvalersi, per il trattamento di dati, anche sensibili, di soggetti pubblici o privati che, in qualità di responsabili del trattamento, forniscano le garanzie di cui al comma 1, stipulando atti giuridici in forma scritta, che specificano la finalità perseguita, la tipologia dei dati, la durata del trattamento, gli obblighi e i diritti del responsabile del trattamento e le modalità di trattamento.

4. Gli atti che disciplinano il rapporto tra il Titolare ed il Responsabile del trattamento devono in particolare contenere quanto previsto dall'art. 28, p. 3, RGPD; tali atti possono anche basarsi su clausole contrattuali tipo adottate dal Garante per la protezione dei dati personali oppure dalla

Commissione europea.

5. E' consentita la nomina di sub-responsabili del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

Il Responsabile risponde, anche dinanzi al Titolare, dell'operato del sub-responsabile (o incaricato del trattamento) anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli è in alcun modo imputabile e che ha vigilato in modo adeguato sull'operato del sub-responsabile.

6. Il Responsabile del trattamento garantisce che chiunque agisca sotto la sua autorità ed abbia accesso a dati personali sia in possesso di apposita formazione ed istruzione e si sia impegnato alla riservatezza od abbia un adeguato obbligo legale di riservatezza.

7. Il Responsabile del trattamento dei dati provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli dal Titolare, analiticamente specificati per iscritto nell'atto di designazione, ed in particolare provvede:

- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Titolare;

- all'adozione di idonee misure tecniche e organizzative adeguate per garantire la sicurezza dei trattamenti;

- alla sensibilizzazione ed alla formazione del personale che partecipa ai trattamenti ed alle connesse attività di controllo;

- alla designazione del Responsabile per la Protezione dei Dati (RPD), se a ciò demandato dal Titolare;

- ad assistere il Titolare nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo allo stesso ogni informazione di cui è in possesso;

- ad informare il Titolare, senza ingiustificato ritardo, della conoscenza di casi di violazione dei dati personali (cd. "*data breach*"), per la successiva notifica della violazione al Garante Privacy, nel caso che il Titolare stesso ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art. 6

Sub- responsabili (o incaricati del trattamento) del procedimento

E' consentita la nomina di sub-responsabili(o incaricati) del trattamento da parte di ciascun Responsabile del trattamento per specifiche attività di trattamento, nel rispetto degli stessi obblighi

contrattuali che legano il Titolare ed il Responsabile primario; le operazioni di trattamento possono essere effettuate solo da incaricati che operano sotto la diretta autorità del Responsabile attenendosi alle istruzioni loro impartite per iscritto che individuano specificatamente l'ambito del trattamento consentito.

La nomina va comunicata al Sindaco che deve essere anche informato di ogni variazione o sostituzione dei sub-responsabili del trattamento.

Art. 7

Responsabili esterni del trattamento.

Il Titolare per il trattamento dei dati, anche sensibili, può avvalersi di soggetti pubblici o privati, che in qualità di responsabili del trattamento stipulano accordi scritti che specificano la finalità perseguita, la tipologia dei dati trattati, la durata del trattamento, gli obblighi e i diritti del Responsabile del trattamento, e le modalità di trattamento.

Ai responsabili esterni si applicano le disposizioni dettate per i responsabili del trattamento all'art. 5 in quanto compatibili.

Art. 8

Responsabile della protezione dei dati

1.Il Responsabile della protezione dei dati (in seguito indicato con "RPD") è individuato nella figura unica dell'avv. Vincenza Pierri .

2. Il Titolare ed il Responsabile del trattamento assicurano che il RPD sia tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali. A tal fine:

- il RPD è invitato a partecipare alle riunioni di coordinamento dei Dirigenti/Responsabili P.O. che abbiano per oggetto questioni inerenti la protezione dei dati personali;

- il RPD deve disporre tempestivamente di tutte le informazioni pertinenti sulle decisioni che impattano sulla protezione dei dati, in modo da poter rendere una consulenza idonea, scritta od orale;

- il parere del RPD sulle decisioni che impattano sulla protezione dei dati è obbligatorio ma non vincolante. Nel caso in cui la decisione assunta determina condotte difformi da quelle raccomandate dal RPD, è necessario motivare specificamente tale decisione;

- il RPD deve essere consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

3. Nello svolgimento dei compiti affidatigli il RPD deve debitamente considerare i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del

medesimo. In tal senso il RPD:

a) procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;

b) definisce un ordine di priorità nell'attività da svolgere - ovvero un piano annuale di attività - incentrandola sulle aree di attività che presentano maggiori rischi in termini di protezione dei dati, da comunicare al Titolare ed al Responsabile del trattamento.

4. Il RPD dispone di autonomia e risorse sufficienti a svolgere in modo efficace i compiti attribuiti, tenuto conto delle dimensioni organizzative e delle capacità di bilancio dell'Ente.

5. La figura di RPD è incompatibile con chi determina le finalità od i mezzi del trattamento; in particolare, risultano con la stessa incompatibili:

- il Responsabile per la prevenzione della corruzione e per la trasparenza;

- il Responsabile del trattamento;

- qualunque incarico o funzione che comporta la determinazione di finalità o mezzi del trattamento.

6. Il Titolare ed il Responsabile del trattamento forniscono al RPD le risorse necessarie per assolvere i compiti attribuiti e per accedere ai dati personali ed ai trattamenti. In particolare è assicurato al RPD:

- supporto attivo per lo svolgimento dei compiti da parte dei Dirigenti/Responsabili P.O. e della Giunta comunale, anche considerando l'attuazione delle attività necessarie per la protezione dati nell'ambito della programmazione operativa (DUP), di bilancio, di Peg e di Piano della performance;

- tempo sufficiente per l'espletamento dei compiti affidati al RPD;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale, ovvero (*in relazione alle dimensioni organizzative dell'Ente*) tramite la costituzione di una U.O., ufficio o gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale);

- comunicazione ufficiale della nomina a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'Ente;

- accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.

7. Il RPD opera in posizione di autonomia nello svolgimento dei compiti allo stesso attribuiti; in particolare, non deve ricevere istruzioni in merito al loro svolgimento né sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Il RPD non può essere rimosso o penalizzato dal Titolare e dal Responsabile del trattamento per

l'adempimento dei propri compiti.

Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Titolare - Sindaco o suo delegato - od al Responsabile del trattamento.

Nel caso in cui siano rilevate dal RPD o sottoposte alla sua attenzione decisioni incompatibili con il RGPD e con le indicazioni fornite dallo stesso RPD, quest'ultimo è tenuto a manifestare il proprio dissenso, comunicandolo al Titolare ed al Responsabile del trattamento.

Art.9

Competenze del Responsabile della protezione dati.

Il RPD è incaricato dei seguenti compiti:

a) informare e fornire consulenza al Titolare ed al Responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. In tal senso il RPD può indicare al Titolare e/o al Responsabile del trattamento i settori funzionali ai quali riservare un *audit* interno o esterno in tema di protezione dei dati, le attività di formazione interna per il personale che tratta dati personali, e a quali trattamenti dedicare maggiori risorse e tempo in relazione al rischio riscontrato;

b) sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati, fermo restando le responsabilità del Titolare e del Responsabile del trattamento. Fanno parte di questi compiti la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità, l'attività di informazione, consulenza e indirizzo nei confronti del Titolare e del Responsabile del trattamento;

c) sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal Titolare e dal Responsabile del trattamento;

d) fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Titolare, in particolare, si consulta con il RPD in merito a: se condurre o meno una DPIA; quale metodologia adottare nel condurre una DPIA; se condurre la DPIA con le risorse interne ovvero esternalizzandola; quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi delle persone interessate; se la DPIA sia stata condotta correttamente o meno e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'art. 36

RGPD, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione. A tali fini il nominativo del RPD è comunicato dal Titolare e/o dal Responsabile del trattamento al Garante;

f) tenuta dei registri;

g) altri compiti e funzioni a condizione che il Titolare o il Responsabile del trattamento si assicurino che tali compiti e funzioni non diano adito a un conflitto di interessi. L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza del RPD.

Art. 10

Trattamento dati particolari

I dati particolari, sensibili ai sensi dell'art. 9 RGPD, che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, biometrici, relativi alla salute, alla vita sessuale ed i dati giudiziari saranno trattati dall'Ente :
– l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche;
– il trattamento è necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale
– il trattamento è necessario per tutelare un interesse vitale dell'interessato;
– per diritti dell'interessato in materia di diritto del lavoro e sicurezza sociale e protezione sociale autorizzato da norma di legge o contratto collettivo;
– il trattamento riguarda dati personali resi manifestamente pubblici dall'interessato;
-il trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri;
– il trattamento è necessario ai fini di archiviazione nel pubblico interesse di ricerca scientifica o storica o a fini statistici ed è proporzionato alla finalità perseguita;
In tutti i casi indicati vanno sempre previste misure di garanzia appropriate e specifiche per tutelare i diritti fondamentali e gli interessati..
I dati particolari riguardanti lo stato di salute non devono essere divulgati.

I dati particolari saranno trattati in modo da assicurarne l'esattezza, la pertinenza, non eccedenza ed indispensabilità rispetto alle finalità perseguite e saranno aggiornati periodicamente.
Le interconnessioni con altre informazioni sensibili e giudiziarie detenute dal Comune avverranno soltanto previa verifica della loro stretta indispensabilità, da valutarsi caso per caso, e con indicazione scritta dei motivi che giustificano tale operazione.
Sono inutilizzabili i dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati

personali

Art. 11

Individuazione di interesse pubblico rilevante

Sono considerati di rilevante interesse pubblico i trattamenti dei dati relativi a:

STATO CIVILE, ANAGRAFE (sia dei residenti in Italia che degli Italiani all'estero) E LISTE ELETTORALI;

CITTADINANZA, IMMIGRAZIONE E CONDIZIONE DELLO STRANIERO;

ESERCIZIO DEI DIRITTI POLITICI E PUBBLICITÀ DELL'ATTIVITÀ DI DETERMINATI ORGANI

RAPPORTI DI LAVORO (in particolare attività finalizzate all'espletamento degli adempimenti previsti per il trattamento economico e giuridico);

MATERIA TRIBUTARIA

BENEFICI ECONOMICI ED ABILITAZIONI

VOLONTARIATO E SERVIZI SOCIALI

ATTIVITÀ DI PREDISPOSIZIONE DI ELEMENTI DI TUTELA I N SEDE AMMINISTRATIVA O GIURISDIZIONALE

RAPPORTI CON ENTI DI CULTO

Art. 12

Pubblicazione web per obblighi di trasparenza

Il Comune di Salerno effettua il trattamento di dati personali, contenuti in atti e documenti amministrativi, che devono essere pubblicati sul web per obblighi di trasparenza previsti dal D.Lgs. n. 33/2013.

Non possono essere resi intellegibili i dati non necessari, eccedenti o non pertinenti con la finalità di pubblicazione.

I dati particolari idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale possono essere diffusi solo se indispensabili; i dati particolari relativi alla

vita sessuale e i dati idonei a rivelare lo stato di salute non possono essere diffusi per finalità di trasparenza.

I dati vanno pubblicati in formato di tipo aperto ai sensi dell'art. 68, D.Lgs. n. 82/2005 e sono liberamente riutilizzabili secondo la normativa vigente. I dati personali diversi dai dati sensibili e dai dati giudiziari, possono essere diffusi attraverso siti istituzionali, nonché trattati secondo modalità che ne consentono la indicizzazione e la rintracciabilità tramite i motori di ricerca web.

I dati, le informazioni e i documenti sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello dell'obbligo di pubblicazione.

Deroghe alla predetta durata temporale quinquennale sono previste:

- nel caso in cui gli atti producono ancora i loro effetti alla scadenza dei cinque anni, con la conseguenza che gli stessi devono rimanere pubblicati fino alla cessazione della produzione degli effetti;
- per alcuni dati e informazioni riguardanti i titolari di incarichi politici, di carattere elettivo o comunque di esercizio di poteri di indirizzo politico, di livello statale regionale e locale ai sensi dell'art. 14, comma 2, D.Lgs. n. 33/2013 e i titolari di incarichi dirigenziali e di collaborazione o consulenza che devono rimanere pubblicati online per i tre anni successivi dalla cessazione del mandato o dell'incarico ai sensi dell'art. 15, comma 4, D.Lgs. n. 33/2013;
- nel caso in cui siano previsti diversi termini dalla normativa in materia di trattamento dei dati personali.

I dati personali devono essere conservati, in ogni caso, per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati; l'interessato ha sempre diritto di ottenere la cancellazione dei dati personali di cui non è necessaria la conservazione in relazione agli scopi per i quali sono stati raccolti o successivamente trattati.

Art. 13

Trattamento dei dati personali effettuato con sistemi di videosorveglianza

In caso di accesso ad area sottoposta, per ragioni di sicurezza, a videosorveglianza (anche in occasioni di spettacoli pubblici), gli interessati devono sempre essere informati ed il trattamento dei dati personali effettuato mediante l'uso di tali sistemi richiede apposita informativa agli interessati che deve essere agevolmente reperibile sia sul sito internet dell'Amministrazione che presso la sede della Polizia Municipale.

In ogni caso il Titolare al fine di fornire oralmente un'informativa adeguata potrà disporre che il

supporto con l'informativa:
– deve essere collocato prima del raggio di azione della telecamera, anche nelle sue immediate vicinanze e non necessariamente a contatto con gli impianti;

– deve avere un formato ed un posizionamento tale d a essere chiaramente visibile in ogni condizione di illuminazione ambientale, anche quando il sistema di videosorveglianza sia eventualmente attivo in orario notturno;

– può inglobare un simbolo o una stilizzazione di esplicita e immediata comprensione, eventualmente diversificati al fine di informare se le immagini sono solo visionate.

La durata della 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 in conformità dell'art. 6, co. 9, D.L. n. 11/2009. Tempi di durata maggiore della conservazione dei dati necessitano di richiesta al Garante adeguatamente motivata con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti (es. collaborazione con l'autorità giudiziaria o dalla polizia giudiziaria in relazione ad un'attività investigativa in corso) .

Art. 14

Misure per dati raccolti con sistemi di videosorveglianza

I dati raccolti mediante sistemi di videosorveglianza devono essere protetti con idonee e preventive misure di sicurezza, riducendo al minimo i rischi di distruzione, di perdita, anche accidentale, di accesso non autorizzato, di trattamento non consentito o non conforme alle finalità della raccolta, anche in relazione alla trasmissione delle immagini.
Occorre rispettare i princìpi di pertinenza e di non eccedenza, raccogliendo solo i dati strettamente necessari per il raggiungimento delle finalità perseguite, registrando le sole immagini indispensabili, limitando l'angolo visuale delle riprese, evitando – quando n on indispensabili – immagini dettagliate, ingrandite o dettagli non rilevanti, e stabilendo in modo conseguente la localizzazione delle telecamere e le modalità di ripresa.
Devono quindi essere adottate almeno le seguenti specifiche misure tecniche ed organizzative

Art. 15
Registro delle attività di trattamento

1. Il Registro delle attività di trattamento svolte dal Titolare del trattamento reca almeno le seguenti

informazioni:

a) il nome ed i dati di contatto del Comune, del Sindaco e/o del suo Delegato eventualmente del Contitolare del trattamento, del RPD;

b) le finalità del trattamento;

c) la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;

d) le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;

e) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

f) ove stabiliti, i termini ultimi previsti per la cancellazione delle diverse categorie di dati;

g) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate;

2. Il Registro è tenuto dal Titolare ovvero dal soggetto dallo stesso delegato, presso gli uffici della struttura organizzativa del Comune in forma telematica/cartacea; nello stesso possono essere inserite ulteriori informazioni tenuto conto delle dimensioni organizzative dell'Ente.

Art.16

Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun Responsabile reca le seguenti informazioni:

a) il nome ed i dati di contatto del Responsabile del trattamento e del RPD;

b) le categorie di trattamenti effettuati da ciascun Responsabile: raccolta, registrazione, organizzazione, strutturazione, conservazione, adattamento o modifica, estrazione, consultazione, uso, comunicazione, raffronto, interconnessione, limitazione, cancellazione, distruzione, profilazione, pseudonimizzazione, ogni altra operazione applicata a dati personali;

c) l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;

d) il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.

2. Il registro è tenuto dal Responsabile del trattamento presso gli uffici della propria struttura organizzativa in forma telematica/cartacea.

3. Il Responsabile del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Responsabile.

4. Il Titolare del trattamento può decidere di affidare al RPD il compito di tenere il Registro, sotto la responsabilità del medesimo Titolare.

5. Il Titolare può decidere di tenere un Registro unico dei trattamenti. In tal caso il Titolare delega la sua tenuta al Responsabile unico del trattamento o, comunque, ad un solo Responsabile del trattamento,

ovvero può decidere di affidare tale compito al RPD, sotto la responsabilità del medesimo Titolare. Ciascun Responsabile del trattamento ha comunque la responsabilità di fornire prontamente e correttamente al soggetto preposto ogni elemento necessario alla regolare tenuta ed aggiornamento del Registro unico.

Art. 17

Diritto di accesso dell'interessato(art.15 GDPR 679/16)

L'interessato ha il diritto, in qualsiasi momento, di ottenere dal Titolare del trattamento la conferma dell'esistenza di un trattamento dei dati personali che lo riguardano. In caso positivo può chiedere l' accesso e acquisire le seguenti informazioni:

a)finalità del trattamento;

b)categoria dei dati oggetto del trattamento;

c)i destinatari o le categorie di destinatari a cui i dati personali sono sati o saranno comunicati;

d)il periodo previsto di conservazione dei dati o se non è possibile indicarlo con precisione, i criteri utilizzati per determinare tale periodo;

e)l'esistenza del diritto di chiedere al titolare la rettifica o cancellazione del dato o la limitazione dei dati o di opporsi al loro trattamento;

f)il diritto di proporre reclamo ad un'Autorità di controllo;

g)qualora i dati non siano stati raccolti presso l'inteessato tutte le informazioni sulla loro origine;

h)l'esistenza di un processo decisionale automatizzato compresa la profilazione dei dati nonché informazioni sulla logica utilizzata e le conseguenze previste per l'interessato.

La domanda deve essere proposta senza particolari formalità e non deve essere motivata. L'esercizio del diritto di accesso è però subordinato all'identificazione dell'interessato.

Il Titolare del trattamento può rispondere oralmente o per iscritto. Se l'interessato presenta richiesta con mezzi elettronici le informazioni sono fornite elettronicamente a meno che l'interessato non abbia richiesto diversamente.

L'istanza deve essere riscontrata non oltre un mese dal ricevimento della richiesta, termine che può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, il titolare deve informare il richiedente indicando non solo la proroga ma anche i motivi del ritardo.

Il rilascio della copia è gratuito; il titolare può addebitare un contributo spese solo in caso di richieste massive.

Art. 18

Diritto alla rettifica (art.16 GDPR 679/16)

L'interessato ha il diritto di ottenere dal Titolare la rettifica dei dati personali inesatti che lo riguardano senza giustificato ritardo.

Il diritto di rettifica previsto dal GDPR è strumento di tutela del più ampio diritto all'identità personale vale a dire del diritto alla veritiera rappresentazione della propria personalità.

La richiesta di rettifica va presentata all'interessato senza particolari formalità e secondo le modalità tradizionali (cartacce, elettroniche o attraverso l'invio di un form web) .

Il titolare è tenuto ad adempiere entro un mese dal ricevimento dell'istanza a meno che – data la complessità della richiesta – non sia necessario un termine più lungo In tal caso potrà disporre la rettifica entro il termine complessivo di tre mesi, previa comunicazione della proroga all'interessato

Il titolare ha l'obbligo di comunicare all'interessato la rettifica dei dati personali.

Art. 19
Diritto alla cancellazione (diritto all'oblio art.17 GDPR 679/16)

L'interessato ha il diritto di ottenere dal Titolare del trattamento la cancellazione dei dati personali che lo riguardano senza ingiustificato ritardo ed il titolare ha l'obbligo di cancellare i dati se sussiste uno dei seguenti motivi:

-i dati personali eccedono le finalità per le quali sono stati raccolti o trattati;

-intervenga revoca del consenso già precedentemente rilasciato (salvo esenzioni e deroghe in caso di trattamento a scopi giornalistici);

-l'interessato esercita il diritto di opposizione (art.21 par. 1 e2);

-l'eliminazione dei dati deriva da un obbligo legale dettato dal diritto dell'UE o di uno Stato membro in cui ha sede il titolare del trattamento;

-i dati sono stati trattati illecitamente;

-i dati sono stati raccolti per finalità legate all'offerta di servizi della società dell'informazione diretti dei minori.

La richiesta di cancellazione va presentata all'interessato senza particolari formalità e secondo le modalità tradizionali (cartacce, elettroniche o attraverso l'invio di un form web) .

Il titolare è tenuto ad adempiere entro un mese dal ricevimento dell'istanza a meno che – data la complessità della richiesta – non sia necessario un termine più lungo In tal caso il termine può essere prorogato di due mesi, previa comunicazione tempestiva della proroga all'interessato.

Per attuare la cancellazione il titolare può provvedere mediante distruzione, anonimizzazione, pseudonimizzazione .

In caso i dati siano stati diffusi pubblicamente anche su siti web, il Titolare del trattamento, tenendo conto dei costi di attuazione, è tenuto ad informare altri titolari che trattano i medesimi dati, della richiesta di cancellazione di qualsiasi link, copia o riproduzione.

In caso in cui i dati non siano diffusi pubblicamente e su siti web il Titolare del trattamento è tenuto ad avvisare i destinatari della cancellazione dei dati, salvo ciò non sia impossibile o richieda uno s forzo

sproporzionato.

Il titolare ha l'obbligo di comunicare all'interessato la cancellazione dei dati personali.

L'inadempienza da parte del titolare è sanzionata, ai sensi dell'art.83, par.5 lett b), fino a 20.000.000 di euro

Art. 20
Diritto di limitazione di trattamento (art.18 GDPR 679/16)

L'interessato, previa richiesta scritta, ha diritto ad ottenere la limitazione del trattamento:

– in caso sia contestata l'esattezza dei dati personali, per il periodo necessario alla verifica da parte del Comune;

– in caso di trattamento illecito, se si oppone alla cancellazione dei dati chiedendo invece che ne sia limitato l'utilizzo;

– in caso di esercizio di opposizione nell'attesa della verifica dei presupposti del relativo diritto.

Il Titolare del trattamento deve fornire risposta entro 30 giorni dal ricevimento della richiesta; tale termine può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisato del differimento entro un mese dall'istanza.

Il Titolare deve comunicare all'interessato la limitazione di trattamento dei dati senza ritardo.

Deve altresì avvisare i destinatari della limitazione dei dati, salvo ciò n on sia impossibile o richieda uno sforzo sproporzionato.

Art. 21
Diritto alla portabilità dei dati (art.20 GDPR 679/16)

L'interessato ha il diritto di ricevere in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano forniti ad un titolare del trattamento qualora:

il trattamento si basi sul consenso

il trattamento sia effettuato con mezzi automatizzati

La richiesta di cancellazione va presentata all'interessato senza particolari formalità e secondo le modalità tradizionali (cartacce, elettroniche).

Il titolare è tenuto ad adempiere entro un mese dal ricevimento dell'istanza a meno che – data la complessità della richiesta – non sia necessario un termine più lungo In tal caso il termine può essere prorogato di due mesi, previa comunicazione tempestiva della proroga all'interessato.

Art. 22

Diritto di opposizione(art.21 GDPR 679/16)

L'interessato può presentare per iscritto richiesta di opposizione al trattamento dei dati personali che lo riguardano per motivi connessi alla sua situazione particolare, inclusa la profilazione.
Il Titolare del trattamento entro trenta giorni fornisce risposta all'interessato a seguito della valutazione della situazione: è consentito l'esercizio del diritto se non esistano comprovati motivi basati su norma di legge per procedere al trattamento prevalenti sugli interessi del richiedente o se si tratta di esercizio o accertamento di un diritto in sede giudiziaria.
Il termine di cui al precedente comma può essere prorogato di due mesi in casi di particolari complessità ma in tal caso, l'interessato va avvisa to del differimento entro un mese dall'istanza.
In ogni comunicazione all'interessato deve essere inserito l'avviso in modo chiaro e separato dal restante contenuto dell'atto che questi può esercitare il diritto all'opposizione.

Art. 23

Contenuto dell'informativa

Il Titolare del trattamento nel momento in cui i dati personali sono ottenuti fornisce all'interessato le seguenti informazioni:
-l'identità e i dati di contatto del Comune Titolare del trattamento e del Responsabile del trattamento;
-i dati di contatto del Responsabile della protezione dei dati;
-le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
-indicazione delle modalità di trattamento (automatizzato o cartaceo;
-indicazione dei destinatari;
-il periodo di conservazione dei dati personali o, se non è possibile, i criteri utilizzati per determinare tale periodo ;
-l'indicazione dei diritti che l'interessato può esercitare, ovvero: accesso, integrazione e rettifica,, eventuale revoca, portabilità, oblio opposizione e reclamo;
-le conseguenze in caso di rifiuto del trattamento o di omessa comunicazione di dati.
L'informativa privacy deve essere fornita per iscritto in formato cartaceo o elettronico, o qualora l'interessato lo richieda espressamente, anche oralmente, previa verifica dell'identità dell'interessato.
Essa va effettuata:
-in caso di dati personali raccolti presso l'interessato prima dell'inizio del trattamento, nel momento della raccolta dei dati;
-in caso di dati personali non ottenuti presso l'interessato:
-entro un termine ragionevole, massimo di un mese dalla raccolta (non registrazione) dei dati;
-nel caso in cui i dati vadano comunicati all'interessato alla prima comunicazione;
-se i dati personali devono essere comunicati ad un altro destinatario, non oltre la prima comunicazione.
Non è necessario fornire l'informativa:
nel caso in cui l'interessato disponga già di tutte le informazioni necessarie;

- nel caso in cui la comunicazione risulta impossibile o implicherebbe uno sforzo sproporzionato; in particolare per il trattamento ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. In tali casi il Titolare del trattamento adotta misure comunque appropriate per tutelare i diritti dell'interessato anche con pubbliche informazioni.

In presenza di un obbligo di legge che impone la riservatezza e segretezza dei dati personali.

Art. 24

Consenso

Il consenso al trattamento dei dati non è richiesto al Comune di Salerno in quanto pubblica amministrazione se agisce per finalità istituzionali.
Il consenso può essere richiesto se il Comune agisce per specifiche finalità diverse da quelle istituzionali
In tal caso il Titolare del trattamento deve essere in grado di dimostrare che l'interessato ha prestato il proprio consenso.
La richiesta di consenso deve essere comprensibile, facilmente accessibile, chiara e semplice.
Il consenso può essere revocato ed in tal caso la revoca non pregiudica la liceità del trattamento già effettuato.

Art.25
Sicurezza del trattamento

1. Il Comune di Salerno quale Titolare del trattamento dei dati e ciascun Responsabile del trattamento mettono in atto misure tecniche ed organizzative adeguate per garantire un livello di sicurezza adeguato al rischio tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, del campo di applicazione, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche.

2. Le misure tecniche ed organizzative di sicurezza da mettere in atto per ridurre i rischi del trattamento ricomprendono: la pseudonimizzazione; la minimizzazione; la cifratura dei dati personali; la capacità di assicurare la continua riservatezza, integrità, disponibilità e resilienza dei sistemi e dei servizi che trattano i dati personali; la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico; una procedura per provare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

3. Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto ciascun Responsabile del trattamento:

- sistemi di autenticazione; sistemi di autorizzazione; sistemi di protezione (antivirus; firewall;

antintrusione; altro);

- misure antincendio; sistemi di rilevazione di intrusione; sistemi di sorveglianza; sistemi di protezione con videosorveglianza; registrazione accessi; porte, armadi e contenitori dotati di serrature e ignifughi; sistemi di copiatura e conservazione di archivi elettronici; altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

4. La conformità del trattamento dei dati al RGDP in materia di protezione dei dati personali è dimostrata attraverso l'adozione delle misure di sicurezza o l'adesione a codici di condotta approvati o ad un meccanismo di certificazione approvato.

5. Il Comune di Salerno e ciascun Responsabile del trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.

6. I nominativi ed i dati di contatto del Titolare, del o dei Responsabili del trattamento e del Responsabile della protezione dati sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.

Art. 26
Valutazione processi per verifica conformità trattamento dati

Il Comune di Salerno al fine di assicurare e garantire che il trattamento dei dati personali è conforme al Regolamento UE 679/2016, tramite il Responsabile della protezione dei dati, mediante audit, che si sostanzia nella somministrazione di questionari ed interviste al responsabile, sub-responsabile ed incaricati, e consultazione delle banche dati ed archivi informatici e cartacei del Comune, opera una valutazione dei processi interni all'ente locale, per verificare il grado di conformità del trattamento dei dati personali effettuato da tutti gli uffici alla normativa vigente, e che tutti i dipendenti osservino le re gole per la liceità e la sicurezza del trattamento di dati personali.
Tutte le fasi del procedimento ed i risultati vengono formalizzati in un rapporto di Audit e fornisce al Comune l'indicazione delle eventuali azioni correttive da porre in essere.

Art. 27

Monitoraggio semestrale del trattamento dei dati

Il Comune di Salerno, con cadenza semestrale, tramite il Responsabile di trattamento verifica l'applicazione delle procedure interne e delle misure di sicurezza adottate in sede di audit e, precisamente che venga assicurato:
– un uso corretto di mezzi informatici nel trattamento dei dati personali monitorando l'utilizzo delle password e gli accessi agli archivi elettronici contenenti dati personali con particolare attenzione ai dati

sensibili;

– un corretto utilizzo degli archivi cartacei che conservano i dati personali con particolare riguardo alla conservazione dei dati sensibili;

– adeguata formazione dei dipendenti in modo diversificato in base alla modalità di trattamento cui sono preposti;

– trattamento de dati secondo il principio di minimizzazione, ovvero, solo a ciò che sia strettamente necessario, esattezza e correttezza dei dati e conservazione dei dati nel rispetto dei termini indicati dalle norme, laddove presenti, o, in subordine per il tempo strettamente necessario al raggiungimento della finalità di trattamento;

– in caso di incidenti o violazioni l'applicazione delle misure correttive per porre riparo agli effetti negativi;

– garantire i diritti degli interessati e corretta valutazione delle istanze di accesso, cancellazione, limitazione del trattamento, rettifica nonché verifica delle istanze di opposizione nonché dei reclami eventualmente presentati al Garante;

– aggiornamento dei contenuti delle informative e adeguamento alle esigenze dei differenti uffici e differenti trattamenti;

– i documenti contenenti dati personali, presenti nel sito internet del Comune, con particolare riferimento alla pubblicazione all'albo pretorio ed alla sezione Amministrazione Trasparente siano conformi ai tempi di pubblicazione previsti dall'art. 124, D.Lgs. n. 267/2000 e D.Lgs. n. 33/2013;

– nelle ipotesi di utilizzo di sistemi di video sorveglianza vengano rispetto delle specifiche misure di sicurezza così come indicate nel presente regolamento.

In caso di riscontro di non corretta applicazione del sistema di audit predisposto e delle norme sul trattamento dei dati personali, il Responsabile di trattamento insieme al Responsabile della Protezione dei dati predispone l'adozione di misure nuove correttive.

Se in sede di monitoraggio semestrale, insieme alla collaborazione del Responsabile della protezione dei dati, si riscontri la possibilità di migliorare ulteriormente il trattamento dei dati effettuato dai vari uffici comunali nell'ottica di obiettivi di efficienza, il Responsabile del trattamento procede nel riesame e nella sostituzione delle misure già applicate.

Art.28

Valutazioni d'impatto sulla protezione dei dati

1. Nel caso in cui un tipo di trattamento, specie se prevede in particolare l'uso di nuove tecnologie, possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il Titolare, prima di effettuare il trattamento, deve attuare una valutazione dell'impatto del medesimo trattamento (DPIA) ai sensi dell'art. 35 RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento. La DPIA è una procedura che permette di realizzare e dimostrare la conformità alle norme del

trattamento di cui trattasi.

2. Ai fini della decisione di effettuare o meno la DPIA si tiene conto degli elenchi delle tipologie di trattamento soggetti o non soggetti a valutazione come redatti e pubblicati dal Garante Privacy ai sensi dell'at. 35, pp. 4-6, RGDP.

3. La DPIA è effettuata in presenza di un rischio elevato per i diritti e le libertà delle persone fisiche. Fermo restando quanto indicato dall'art. 35, p. 3, RGDP, i criteri in base ai quali sono evidenziati i trattamenti determinanti un rischio intrinsecamente elevato, sono i seguenti:

a) trattamenti valutativi o di *scoring*, compresa la profilazione e attività predittive, concernenti aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato;

b) decisioni automatizzate che producono significativi effetti giuridici o di analoga natura, ossia trattamenti finalizzati ad assumere decisioni su interessati che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche;

c) monitoraggio sistematico, ossia trattamenti utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza sistematica di un'area accessibile al pubblico;

d) trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;

e) trattamenti di dati su larga scala, tenendo conto: del numero di numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento; volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento; durata o persistenza dell'attività di trattamento; ambito geografico dell'attività di trattamento;

f) combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;

g) dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela per il quale si possa identificare una situazione di disequilibrio nel rapporto con il Titolare del trattamento, come i dipendenti dell'Ente, soggetti con patologie psichiatriche, richiedenti asilo, pazienti, anziani e minori;

h) utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

i) tutti quei trattamenti che, di per sé, impediscono agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto.

Nel caso in cui un trattamento soddisfi almeno due dei criteri sopra indicati occorre, in via generale,

condurre una DPIA, salvo che il Titolare ritenga motivatamente che non può presentare un rischio elevato; il Titolare può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

4. Il Titolare garantisce l'effettuazione della DPIA ed è responsabile della stessa. Il Titolare può affidare la conduzione materiale della DPIA ad un altro soggetto, interno o esterno al Comune.

Il Titolare deve consultarsi con il RPD anche per assumere la decisione di effettuare o meno la DPIA; tale consultazione e le conseguenti decisioni assunte dal Titolare devono essere documentate nell'ambito della DPIA. Il RPD monitora lo svolgimento della DPIA.

Il Responsabile del trattamento deve assistere il Titolare nella conduzione della DPIA fornendo ogni informazione necessaria.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, forniscono supporto al Titolare per lo svolgimento della DPIA.

5. Il RPD può proporre lo svolgimento di una DPIA in rapporto a uno specifico trattamento, collaborando al fine di mettere a punto la relativa metodologia, definire la qualità del processo di valutazione del rischio e l'accettabilità o meno del livello di rischio residuale.

Il responsabile della sicurezza dei sistemi informativi, se nominato, e/o l'ufficio competente per detti sistemi, possono proporre di condurre una DPIA in relazione a uno specifico trattamento, con riguardo alle esigenze di sicurezza od operative.

6. La DPIA non è necessaria nei casi seguenti:

1 se il trattamento non può comportare un rischio elevato per i diritti e le libertà di persone fisiche ai sensi dell'art. 35, p. 1, RGDP;

2 se la natura, l'ambito, il contesto e le finalità del trattamento sono simili a quelli di un trattamento per il quale è già stata condotta una DPIA. In questo caso si possono utilizzare i risultati della DPIA svolta per l'analogo trattamento;

3 se il trattamento è stato sottoposto a verifica da parte del Garante Privacy prima del maggio 2018 in condizioni specifiche che non hanno subito modifiche;

4 se un trattamento trova la propria base legale nella vigente legislazione che disciplina lo specifico trattamento, ed è già stata condotta una DPIA all'atto della definizione della base giuridica suddetta.

Non è necessario condurre una DPIA per quei trattamenti che siano già stati oggetto di verifica preliminare da parte del Garante della Privacy o da un RDP e che proseguano con le stesse modalità oggetto di tale verifica. Inoltre, occorre tener conto che le autorizzazioni del Garante Privacy basate

sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite od abrogate.

Art.29

Procedimento DPIA

La DPIA è condotta prima di dar luogo al trattamento, attraverso i seguenti processi:

a) descrizione sistematica del contesto, dei trattamenti previsti, delle finalità del trattamento e tenendo conto dell'osservanza di codici di condotta approvati. Sono altresì indicati: i dati personali oggetto del trattamento, i destinatari e il periodo previsto di conservazione dei dati stessi; una descrizione funzionale del trattamento; gli strumenti coinvolti nel trattamento dei dati personali (hardware, software, reti, persone, supporti cartacei o canali di trasmissione cartacei);

b) valutazione della necessità e proporzionalità dei trattamenti, sulla base:

- delle finalità specifiche, esplicite e legittime;
- della liceità del trattamento;
- dei dati adeguati, pertinenti e limitati a quanto necessario;
- del periodo limitato di conservazione;
- delle informazioni fornite agli interessati;
- del diritto di accesso e portabilità dei dati;
- del diritto di rettifica e cancellazione, di opposizione e limitazione del trattamento;
- dei rapporti con i responsabili del trattamento;
- delle garanzie per i trasferimenti internazionali di dati;
- consultazione preventiva del Garante privacy;

c) valutazione dei rischi per i diritti e le libertà degli interessati, valutando la particolare probabilità e gravità dei rischi rilevati. Sono determinati l'origine, la natura, la particolarità e la gravità dei rischi o, in modo pii specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;

d) individuazione delle misure previste per affrontare ed attenuare i rischi, assicurare la protezione dei dati personali e dimostrare la conformità del trattamento con il RGPD, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Il Titolare può raccogliere le opinioni degli interessati o dei loro rappresentanti, se gli stessi possono

essere preventivamente individuati. La mancata consultazione è specificatamente motivata, così come la decisione assunta in senso difforme dall'opinione degli interessati.

La DPIA deve essere effettuata - con eventuale riesame delle valutazioni condotte - anche per i trattamenti in corso che possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, nel caso in cui siano intervenute variazioni dei rischi originari tenuto conto della natura, dell'ambito, del contesto e delle finalità del medesimo trattamento.

E' pubblicata sul sito istituzionale dell'Ente, in apposita sezione, una sintesi delle principali risultanze del processo di valutazione ovvero una semplice dichiarazione relativa all'effettuazione della DPIA.

Art.30

Consultazione del Garante della privacy

Il Titolare deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. Il Titolare consulta il Garante Privacy anche nei casi in cui la vigente legislazione stabilisce l'obbligo di consultare e/o ottenere la previa autorizzazione della medesima autorità, per trattamenti svolti per l'esecuzione di compiti di interesse pubblico, fra cui i trattamenti connessi alla protezione sociale ed alla sanità pubblica.

Il Comune di Salerno tramite il Responsabile della protezione dei dati ai sensi degli artt. 36 e 39, par. 1, lett. e), Regolamento UE n. 679/2016, invia richiesta di consultazione al Garante comunicando:

-i dati dell'ente locale in quanto Titolare del trattamento ed i propri dati in quanto punto di contatto e referente per la consultazione;

– le finalità ed i mezzi di trattamento previsti;

– le misure di garanzia previste per proteggere i diritti e le libertà fondamentali degli interessati;

– la valutazione di impatto sulla protezione dei da ti in versione completa;

– ogni altra informazione ritenuta necessaria.

Il Garante formula parere scritto entro otto settimane dal ricevimento della richiesta di consultazione nel caso in cui ritenga che il trattamento comunicato violi le norme sulla protezione dei dati ed in particolare qualora ritenga che il Comune non abbia sufficientemente attenuato o identificato il rischio. In base alla complessità del trattamento previsto il Garante può prorogare la sua risposta di un termine aggiuntivo di sei settimane informando il Responsabile della protezione dei dati, entro un mese dal ricevimento della richiesta di consultazione.

In caso sia necessario il Garante può richiedere al Responsabile della protezione dei dati informazioni aggiuntive a quelle già comunicate e p uò sospendere la decorrenza dei termini di cui al c omma 3 in attesa della loro trasmissione.

In assenza di parere espresso del Garante entro le otto settimane dal ricevimento della richiesta di consultazione, il Comune può procedere nel trattamento dei dati.

Art. 31

Violazione dei dati personali

Per violazione dei dati personali (in seguito "*data breach*") si intende la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato ai dati personali trasmessi, conservati o comunque trattati dal Comune.

Il Titolare, ove ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati, provvede alla notifica della violazione al Garante Privacy. La notifica dovrà avvenire entro 72 ore e comunque senza ingiustificato ritardo. Il Responsabile del trattamento è obbligato ad informare il Titolare, senza ingiustificato ritardo, dopo essere venuto a conoscenza della violazione.

I principali rischi per i diritti e le libertà degli interessati conseguenti ad una violazione, in conformità al considerando 75 del RGPD, sono i seguenti:

- danni fisici, materiali o immateriali alle persone fisiche;

- perdita del controllo dei dati personali;

- limitazione dei diritti, discriminazione;

- furto o usurpazione d'identità;

- perdite finanziarie, danno economico o sociale.

- decifratura non autorizzata della pseudonimizzazione;

- pregiudizio alla reputazione;

- perdita di riservatezza dei dati personali protetti da segreto professionale (sanitari, giudiziari).

Se il Titolare ritiene che il rischio per i diritti e le libertà degli interessati conseguente alla violazione rilevata è elevato, allora deve informare questi ultimi, senza ingiustificato ritardo, con un linguaggio semplice e chiaro al fine di fare comprendere loro la natura della violazione dei dati personali verificatesi. I rischi per i diritti e le libertà degli interessati possono essere considerati "elevati" quando la violazione può, a titolo di esempio:

- coinvolgere un rilevante quantitativo di dati personali e/o di soggetti interessati;

- riguardare categorie particolari di dati personali;

- comprendere dati che possono accrescere ulteriormente i potenziali rischi (ad esempio dati di localizzazione, finanziari, relativi alle abitudini e preferenze);

- comportare rischi imminenti e con un'elevata probabilità di accadimento (ad esempio rischio di perdita finanziaria in caso di furto di dati relativi a carte di credito);

- impattare su soggetti che possono essere considerati vulnerabili per le loro condizioni (ad esempio utenti deboli, minori, soggetti indagati).

La notifica deve avere il contenuto minimo previsto dall'art. 33 RGPD, ed anche la comunicazione all'interessato deve contenere almeno le informazioni e le misure di cui al citato art. 33.

Il Titolare deve opportunamente documentare le violazioni di dati personali subite, anche se non comunicate alle autorità di controllo, nonché le circostanze ad esse relative, le conseguenze e i provvedimenti adottati o che intende adottare per porvi rimedio. Tale documentazione deve essere

conservata con la massima cura e diligenza in quanto può essere richiesta dal Garante Privacy al fine di verificare il rispetto delle disposizioni del RGPD.

Il Titolare del trattamento annota la violazione nel Registro delle violazioni, che contiene tra le altre informazioni: l'ufficio dell'ente locale competente al trattamento dei dati violati, la descrizione e la gravità del data breach, l'indicazione dei dispositivi cartacei o automatizzati coinvolti, la categoria dei dati violati e dei destinatari, le misure di sicurezza presenti ed applicate ai dati violati e le ulteriori eventuali misure adottate.

La documentazione è a disposizione di eventuali ispezioni e verifiche da parte del Garante privacy.

Art.32

Data breach e proedimento

Il Responsabile del trattamento in caso venga a conoscenza della violazione informa senza ingiustificato ritardo il Titolare del trattamento e richiede immediato parere al Responsabile della protezione dei dati sulla gravità della violazione, ovvero:
– se questa sia inoffensiva per le misure di sicurezza già presenti in questo ente;
– se può comportare rischi per gli interessati al trattamento ed il grado dei rischi;
– le misure di sicurezza eventualmente da adottare per porre rimedio alla violazione.
Il Responsabile del trattamento relaziona immediatamente al Titolare del trattamento la violazione indicando la categoria di dati violati ed allega il parere del Responsabile della protezione dei dati in cui viene indicato se le misure presenti nel Comune rendono la violazione inoffensiva o, se invece, vanno integrate.

Al Titolare del trattamento compete la valutazione finale sulla gravità o meno della violazione. In caso venga riscontrata la presenza di rischi per le persone fisiche va effettuata via Pec la notifica del data breach al Garante per la privacy entro 72 ore dal momento in cui ne è venuto a conoscenza o, se in un momento successivo, nel provvedimento vanno indicati i motivi del ritardo.

Art. 33

Notifica al Garante della privacy della violazione

La Notifica al Garante non è necessaria se la violazione è inoffensiva, cioè vi è assenza di rischio per interessati e persone fisiche e ciò si verifica se il Comune pone in essere le misure di sicurezza che rendono i dati inintellegibili perché per esempio anonimi o cifrati in modo sicuro attraverso un algoritmo standardizzato o mediante schemi di cifratura a chiave simmetrica.

Non ricorre l'inintellegibilità se la violazione ha portato la distruzione o perdita dei dati personali.

La notifica al Garante deve presentare il seguente contenuto minimo:

– la natura della violazione dei dati personali le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
– il nome e i dati di contatto del Responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
– le probabili conseguenze della violazione dei dati personali;
– le misure adottate o di cui si propone l'adozione da parte del Comune per porre rimedio alla violazione dei dati personali.

A questo contenuto minimo è possibile aggiungere ogni altra informazione che il Titolare ritiene necessaria.

In caso non si sia in possesso delle informazioni di cui al comma 3 il Titolare procederà a comunicare entro 72 ore quelle di cui è a conoscenza e successivamente, appena verrà in possesso dei dati mancanti effettuerà una comunicazione integrativa senza ingiustificato ritardo.

Il Garante può indicare l'adozione di misure integrative a quelle già descritte nella notifica, oltre che fornire osservazioni per porre rimedio alla violazione e può anche imporre la comunicazione all'interessato di cui al successivo articolo, qualora non sia stata ritenuta necessaria dal Comune.

Art. 34

Soggetti responsabili ed azione risarcitoria

Il Comune di Salerno è Responsabile per ogni danno materiale o immateriale causato da una violazione dei dati personali trattati ed è tenuto a risarcire l'interessato o la persona fisica danneggiata.
All'obbligazione risarcitoria è tenuto verso il danneggiato anche il Responsabile del trattamento se il danno è stato causato da un suo inadempimento nell'ambito dei compiti a cui è stato preposto.
Il Titolare del trattamento ed il Responsabile del trattamento vanno esenti da responsabilità se provano che l'evento dannoso non è loro imputabile.
L'azione risarcitoria va proposta dinanzi all'autorità giudiziaria ordinaria secondo le norme dell'ordinamento interno.
Il Responsabile della Protezione dei dati non risponde nei confronti dei danneggiati ma solo nei confronti del Comune Titolare del trattamento ed in relazione alle specifiche competenze attribuite al momento del conferimento dell'incarico e con successivi accordi scritti.

Art. 35
Reclamo

Fatta salva la tutela giurisdizionale l'interessato può presentare reclamo al Garante se ritiene che il Comune abbia violato la riservatezza dei propri dati.
Il reclamo è presentato in forma scritta senza particolari formalità al Garante e contiene la documentazione utile per la valutazione nonché le informazioni sul Comune e sul Responsabile di trattamento oltre che dell'interessato.
Il Garante effettua un'istruttoria preliminare in cui può richiedere informazioni al Comune ed all'esito del procedimento può imporre al Comune di adottare i provvedimenti necessari per rendere il trattamento dei dati conforme alla disciplina vigente.
Il Garante informa l'interessato dello stato o dell'esito di reclamo.

Art. 36

Trattamento illecito dei dati (art 167 dlgs 196/2003)

Salvo che il fatto costituisca più grave reato, chiunque, al fine di trarne per sé o per altri profitto o di recare danno all'interessato, effettua un trattamento di dati personali in violazione delle norme sulla protezione dei dati personali, è punito, con il sistema sanzionatorio per come previsto dall'art. 167 dlgs 196/2003 .

Art. 37

Falsità nelle dichiarazioni e notificazioni al Garante della privacy(art.168 Dlgs 196/2003)

Salvo che il fatto costituisca più grave reato, chiunque in un procedimento o nel corso di accertamento dinanzi al Garante dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi, è punito con la reclusione da sei mesi a tre anni.

E' punito con la reclusione fino ad un anno chiunque, intenzionalmente, cagiona un'interruzione o turba la regolarità di un procedimento dinanzi al garante o degli accertamenti dallo stesso svolti.

Art. 38

Entrata in vigore del regolamento

Il presente regolamento entra in vigore il giorno in cui diviene esecutiva la relativa delibera di approvazione.

Il regolamento e la relativa modulistica per l'esercizio dei diritti sono resi pubblici mediante pubblicazione sul sito internet del Comune, nella Sezione Amministrazione Trasparente.

Copia del regolamento va inoltrata al Segretario comunale ed ai responsabili di servizio, al RPD, al Responsabile del trattamento, ai sub-responsabili ed ogni altro dipendente che tratta dati personali nel Comune.

Art. 39
Rinvio

Per tutto quanto non espressamente disciplinato con le presenti disposizioni, si applicano le disposizioni del RGPD e tutte le sue norme attuative vigenti.