Città di
CAIRO
Montenotte

Deliberazione del Consiglio Comunale - copia

SESSIONE IN **SEDUTA STRAORDINARIA** di prima convocazione

Deliberazione N. 36 del 25 MAGGIO 2018

ADOZIONE DEL REGOLAMENTO COMUNALE DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Ai sensi dell'art. 11 del Regolamento per il funzionamento del Consiglio Comunale, si è riunito il Consiglio Comunale in sessione straordinaria pubblica nella sala delle adunanze oggi 25 maggio alle ore 20,30 previo inoltro di invito consegnato a mezzo di posta elettronica certificata.

Presiede la seduta Paolo Lambertini nella sua qualità di Sindaco/Presidente del Consiglio.

Al momento della seduta cui si riferisce la presente delibera risultano:

			Presenti	Assenti
1	-	LAMBERTINI Paolo	X	
2	-	BELTRAME ROBERTA	X	
3	-	BRIANO Maurizio	X	
4	-	DALLA VEDOVA Matteo	X	
5	-	DOGLIOTTI Marco	X	
6	-	FERRARI Giorgia	X	
7	-	FERRARI Nella	X	
8	-	GARRA Caterina	X	
9		GHIONE Fabrizio	X	
10	-	GRANATA Ambra	X	
11	-	LIGORIO Giovanni	X	
12	-	PENNINO Matteo	X	
13	-	PERA Francesca	X	
14	-	PIEMONTESI Ilaria	X	
15	-	POGGIO Alberto	X	
16	-	SPERANZA Roberto	X	
17	-	ZUNINO Nicolo'	X	
			17	—

Risulta giustificata l'assenza del Consigliere Comunale di cui ai nr. ===

Il Segretario Generale dott. Isabella Cerisola partecipa alla seduta e redige il verbale.

Il Presidente, constatato il numero legale degli intervenuti, invita i presenti alla trattazione dell'argomento in oggetto indicato.

Nr. 36

ADOZIONE DEL REGOLAMENTO COMUNALE DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

Relazione del Sindaco

Il Regolamento Generale sulla Protezione dei dati personali (Regolamento UE 679/2016 - di seguito indicato "RGPD") è un atto con il quale la Commissione europea intende rafforzare e rendere più omogenea la protezione dei dati personali dei cittadini, sia all'interno che all'esterno dei confini dell'Unione europea. Il testo diventa definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018.

Il RGPD è parte del cosiddetto "Pacchetto protezione dati personali", l'insieme normativo che definisce un nuovo quadro comune in materia di tutela dei dati personali per tutti gli Stati membri dell'UE.

Nell'ambito del nuovo quadro normativo che la Commissione europea ha voluto delineare e al quale gli Stati membri devono conformarsi, l'Italia ha recepito i nuovi principi attraverso l'art. 13 della legge n. 163/2017 entrata in vigore il 21 novembre 2017, che ha attribuito al Governo la delega ad adottare (entro 6 mesi) uno o più provvedimenti rivolti a:

- abrogare le disposizioni del Decreto Legislativo n. 196/2003 (l'attuale Codice Privacy) che siano in contrasto o comunque incompatibili con la nuova disciplina europea in tema di trattamento di dati personali e a modificarlo al fine di dare puntuale attuazione alle disposizioni del RGPD;

- valutare l'opportunità di avvalersi dei poteri specifici del Garante per la protezione dei dati personali (di seguito Garante Privacy) affinché adotti provvedimenti attuativi e integrativi volti al perseguimento delle finalità previste dal RGPD;

- adeguare l'attuale regime sanzionatorio, a livello penale e amministrativo, alle disposizioni del RGPD, al fine di garantire la corretta osservanza della nuova normativa.

Tali decreti legislativi non sono stati ancora approvati in questa legislatura, tuttavia si sottolinea che essendo il Regolamento europeo direttamente applicabile in tutti gli

Stati membri, dal 25 maggio 2018 la nuova disciplina in materia di privacy entrerà comunque in vigore.

Dunque, per un adeguamento coerente dell'intera nuova disciplina prevista dal Regolamento UE, occorrerà comunque attendere l'emanazione dei suddetti decreti legislativi e delle indicazioni del Garante Privacy.

Pertanto, nelle more del completamento del nuovo assetto ordinamentale in materia, il presente regolamento rappresenta per il Comune la prima concreta attuazione della nuova disciplina vigente in materia di protezione dei dati personali.

Non verificandosi interventi;

IL CONSIGLIO COMUNALE

RICHIAMATO l'art. 42, c.2, lett. a), D.Lgs. 18 agosto 2000 n.267;

PRESO ATTO:

che il Parlamento europeo ed il Consiglio in data 27.4.2016 hanno approvato il Regolamento UE 679/2016 (GDPR- *General Data Protection Regulation)* relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che abroga la direttiva 95/46/CE e che mira a garantire una disciplina uniforme ed omogenea in tutto il territorio dell'Unione europea;

- che il testo, pubblicato nella Gazzetta Ufficiale dell'Unione Europea (GUUE) il 4 maggio 2016, diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018, dopo un periodo di transizione di due anni, in quanto non richiede alcuna forma di legislazione applicativa o attuativa da parte degli stati membri;

- che il Garante per la protezione dei dati personali ha emanato una Guida all'applicazione del Regolamento europeo in materia di protezione dei dati personali che intende offrire un panorama delle principali problematiche che i soggetti pubblici, oltre alle imprese, dovranno tenere presenti in vista della piena applicazione del Regolamento, prevista il 25 maggio 2018;

- che ai sensi dell'art.13 della Legge n.163/2017 il Governo è stato delegato ad adottare, entro sei mesi dalla sua entrata in vigore, uno o più decreti legislativi al fine di adeguare il quadro normativo nazionale alle disposizioni del Regolamento (UE) 2016/679 del 27 aprile 2016 di che trattasi;

RILEVATO:

- che le norme introdotte dal Regolamento UE 2016/679 si traducono in obblighi organizzativi, documentali e tecnici che tutti i Comuni devono, fin da subito, considerare e tenere presenti per consentire la piena e consapevole applicazione del nuovo quadro normativo in materia di privacy entro il 25 maggio 2018;

- che appare necessario ed opportuno stabilire modalità organizzative, misure procedimentali e regole di dettaglio, finalizzate anche ad omogeneizzare questioni interpretative, che permettano a questo Ente di poter agire con adeguata funzionalità ed efficacia nell'attuazione delle disposizioni introdotte dal nuovo Regolamento UE;

VISTO lo schema di Regolamento allegato;

RITENUTO pertanto opportuno procedere alla sua approvazione per permettere a questa Amministrazione di provvedere con immediatezza all'attuazione del Regolamento UE 2016/679;

VISTO il parere di regolarità tecnica del dirigente Finanziaria ai sensi dell'art. 49, Tuel;

ALLA unanimità, espressa per alzata di mano dia 17 Componenti del Consiglio presenti e votanti;

DELIBERA

- Di approvare il Regolamento attuativo del Regolamento UE 2016/679 in materia di protezione dati personali che viene allegato al presente atto per costituirne parte integrante e sostanziale;

- Di dare atto che si procede secondo la disciplina contenuta nel presente atto ed in conformità a quanto stabilito nel Regolamento UE 2016/679 ed in particolare:

- alla nomina dei Responsabili del trattamento;

- alla designazione del Responsabile della Protezione Dati;

- all'istituzione dei registri delle attività di trattamento;

- a mettere in atto misure tecniche e organizzative adeguate per garantire ed essere in grado di dimostrare che i trattamenti dei dati personali vengono effettuati in conformità alla disciplina europea;

- all'aggiornamento della documentazione in essere nell'Ente in relazione ai trattamenti dei dati personali;

Successivamente

Il Consiglio Comunale

RAVVISATA l'opportunità di dare quanto prima operatività alle direttive, in ossequio alle indicazioni legislative;

CON VOTI unanimi espressi per alzata di mano dai 17 Componenti del Consiglio presenti e votanti;

DELIBERA

presente deliberazione è dichiarata immediatamente esecutiva.

Città di
CAIRO
Montenotte

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

Indice

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 Cairo Montenotte.

Art.2
Titolare del Trattamento Dati e Responsabili Trattamento Dati (RTD)

Il Comune di Cairo Montenotte , 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.

Il Comune di Cairo Montenotte 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.

Il Comune di Cairo Montenotte 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.

Il Comune di Cairo Montenotte adotta misure appropriate per fornire all'interessato:

- le informazioni indicate dall'art. 13 RGPD, qualora i dati personali siano raccolti presso lo stesso interessato;
- le informazioni indicate dall'art. 14 RGPD, qualora i dati personali non stati ottenuti presso lo stesso interessato.

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, è necessario 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, tenuto conto di quanto indicato dal successivo art. 9.

6. I Dirigenti delle singole strutture in cui si articola l'organizzazione comunale, sono preposti al trattamento dei dati contenuti nelle banche dati esistenti nelle articolazioni organizzative di loro competenza ed operano quali Responsabili del trattamento Dati, successivamente identificati con l'acronimo RTD. L'elenco degli RTD delle strutture in cui si articola l'organizzazione dell'Ente viene pubblicato in apposita sezione del sito istituzionale ed aggiornandolo periodicamente.

7. Nel caso di servizio associato con altri Comuni, l'RTD è il Dirigente del Comune designato quale Ente capofila del servizio interessato.

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 degli RTD.

Art.3
Finalità del trattamento

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

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.
- l'adempimento di un obbligo legale al quale è soggetto il Comune;
- l'esecuzione di un contratto con soggetti interessati;
- per specifiche finalità diverse da quelle di cui ai precedenti punti, purché l'interessato esprima il consenso al trattamento.

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

Art.4
Responsabile Unico Interno del Trattamento (RUIT)

1. Il Sindaco con proprio decreto nomina il Responsabile Unico Interno del Trattamento, (di seguito identificato con l'acronimo RUIT) di tutte le banche dati personali esistenti nell'articolazione organizzativa di rispettiva competenza. Il RUIT 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. Il RUIT provvede, per il proprio ambito di competenza, a tutte le attività previste dalla legge e a tutti i compiti affidatigli ed in particolare provvede:
- alla tenuta del registro delle categorie di attività di trattamento svolte per conto del Comune;
- 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;
- ad assistere nella conduzione della valutazione dell'impatto sulla protezione dei dati (di seguito indicata con "DPIA") fornendo ogni informazione di cui è in possesso;
- ad informare il Sindaco e l'RPD, 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 in cui si ritenga probabile che dalla violazione dei dati possano derivare rischi per i diritti e le libertà degli interessati.

Art.5
Responsabile della Protezione Dati (RPD)

1. Il Responsabile della protezione dei dati (in seguito indicato con l'acronimo RPD), per la particolarità tecnica della funzione e per la necessità della continua informazione e aggiornamento che non può essere garantita da personale interno dell'Ente, è figura esterna scelto tra professionisti tramite procedura ad evidenza pubblica .
I compiti attribuiti al RPD sono indicati in apposito contratto di servizio. Il RPD è tenuto a mantenere la propria conoscenza specialistica mediante adeguata, specifica e periodica formazione, con onere di comunicazione di detto adempimento al Comune.

Il RPD è incaricato dei seguenti compiti:

- informare e fornire consulenza al RUIT e ai RTD 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 RUIT 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;
- sorvegliare l'osservanza del RGPD e delle altre normative relative alla protezione dei dati. 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 RUIT e degli RTD e del personale preposto al trattamento;
- sorvegliare sulle attribuzioni delle responsabilità, sulle attività di sensibilizzazione, formazione e controllo poste in essere dal RUIT, dagli RTD e del personale preposto al trattamento;
- fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA) e sorvegliarne lo svolgimento. Il Sindaco, 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;
- 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 dal Responsabile Unico Interno del trattamento al Garante;
- la tenuta dei registri di cui ai successivi artt. 7 e 8.

2. Il RUIT assicura 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 degli RTD 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:

- procede ad una mappatura delle aree di attività valutandone il grado di rischio in termini di protezione dei dati;
- 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. 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 RUIT;
- il Personale preposto al trattamento.
E' 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;
-accesso garantito ai settori funzionali dell'Ente così da fornirgli supporto, informazioni e input essenziali.
Il RPD non può essere rimosso o penalizzato dall'Ente per l'adempimento dei propri compiti.
Ferma restando l'indipendenza nello svolgimento di detti compiti, il RPD riferisce direttamente al Sindaco.

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 Sindaco ed al RUIT.

Art.6
Sicurezza del trattamento

Il Comune di Cairo Montenotte mette in atto le 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.
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.
Costituiscono misure tecniche ed organizzative che possono essere adottate dal Servizio cui è preposto il personale addetto al 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.
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.
Il RUIT e il personale preposto al trattamento si obbligano ad impartire adeguate istruzioni sul rispetto delle predette misure a chiunque agisca per loro conto ed abbia accesso a dati personali.
I nominativi ed i dati di contatto del Sindaco,quale rappresentante del Comune Titolare, del RUIT, del RPD e dei RTD sono pubblicati sul sito istituzionale del Comune, sezione Amministrazione trasparente, oltre che nella sezione "privacy" eventualmente già presente.
Restano in vigore le misure di sicurezza attualmente previste per i trattamenti di dati sensibili per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22, D.Lgs. n. 193/2006).

Art.7
Registro delle attività di trattamento

1. Viene istituito il Registro delle attività di trattamento che deve contenere le seguenti informazioni:

- il nome ed i dati di contatto del Comune, del Sindaco o del suo Delegato ai sensi del precedente art.2;
- del RUIT;
- del RPD;
- le finalità del trattamento;
- la sintetica descrizione delle categorie di interessati, nonché le categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati;
- il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate, come da precedente art.6.

2. Il Registro è tenuto dal RUIT in forma telematica/cartacea, secondo lo schema che verrà approvato dal Comune sentiti il RUIT e l'RPD. Nello stesso possono essere inserite ulteriori informazioni.

Art.8
Registro delle categorie di attività trattate

1. Il Registro delle categorie di attività trattate da ciascun RTD di cui al precedente art. 3, reca le seguenti informazioni:
il nome ed i dati di contatto del RUIT del RPD;
le categorie di trattamenti effettuati da ciascun RTD: 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;
l'eventuale trasferimento di dati personali verso un paese terzo od una organizzazione internazionale;
il richiamo alle misure di sicurezza tecniche ed organizzative del trattamento adottate.
2. Il registro è tenuto dal RTD presso gli uffici della propria struttura organizzativa in forma telematica/cartacea, secondo lo schema che verrà approvato dal Comune sentiti il RUIT e l'RPD.

Art.9
Valutazioni d'impatto sulla protezione dei dati

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 RTD, sentito l'RPD, 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.
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.
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:

- 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;
- 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;
- 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;
- trattamenti di dati sensibili o dati di natura estremamente personale, ossia le categorie particolari di dati personali di cui all'art. 9, RGDP;
- 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;
- combinazione o raffronto di insiemi di dati, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato;
- dati relativi a interessati vulnerabili, ossia ogni interessato particolarmente vulnerabile e meritevole di specifica tutela come soggetti con patologie psichiatriche, pazienti, anziani e minori;
- utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative;

- 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 l'RTD, sentito l'RPD, ritenga motivatamente che non può presentare un rischio elevato; l'RTD può motivatamente ritenere che per un trattamento che soddisfa solo uno dei criteri di cui sopra occorra comunque la conduzione di una DPIA.

L'RTD garantisce l'effettuazione della DPIA ed è responsabile della stessa.

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

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.

La DPIA non è necessaria nei casi seguenti:

- 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;
- 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;
- 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;
- 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 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.

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

- 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);

- 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;
- 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 più specifico, di ogni singolo rischio (accesso illegittimo, modifiche indesiderate, indisponibilità dei dati) dal punto di vista degli interessati;
- 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.

L'RTD 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.

L'RTD deve consultare il Garante Privacy prima di procedere al trattamento se le risultanze della DPIA condotta indicano l'esistenza di un rischio residuale elevato. L'RTD 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. 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.

Art. 10
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.

L'RPD, 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. L'RTD o il RUIT sono obbligati ad informare l'RPD, 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 l'RPD 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.

L'RPD 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.

Art.11
Rinvio

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

PARERE DI REGOLARITA' TECNICA
(art. 49 D.lgs nr 267 del 18 agosto 2000)

SU DELIBERAZIONE AD OGGETTO:

ADOZIONE DEL REGOLAMENTO COMUNALE DI ATTUAZIONE DEL REGOLAMENTO UE 2016/679 RELATIVO ALLA PROTEZIONE DELLE PERSONE FISICHE CON RIGUARDO AL TRATTAMENTO DEI DATI PERSONALI

IL DIRIGENTE
RESPONSABILE DEL SERVIZIO FINANZIARIO

Si rilascia parere favorevole sul profilo della regolarità tecnica.

Cairo Montenotte, li 16/5/2018

Andrea Marenco

Letto, confermato e sottoscritto.

IL PRESIDENTE	IL SEGRETARIO GEN.LE
F.to P. LAMBERTINI	F.to I. CERISOLA

REFERTO DI PUBBLICAZIONE

Il sottoscritto Istruttore incaricato attesta che copia della presente deliberazione viene pubblicata all'Albo Pretorio on line del Comune il giorno 31 maggio 2018 vi rimarrà per 15 giorni interi e consecutivi ai sensi dell'art. 124 - 1° comma - del D.Lgs 18/08/2000, nr. 267.

Cairo Montenotte, li 31 maggio 2018

L'ISTRUTTOREAMMINISTRATIVO
F.to M. GARABELLO

La presente Deliberazione è dichiarata [X] **IMMEDIATAMENTE ESECUTIVA**

CERTIFICATO DI ESECUTIVITÀ
(Art. 134, 3° comma, del D.Lgs. 18/08/2000 - nr. 267)

La presente deliberazione è divenuta esecutiva il

Cairo Montenotte, li **IL SEGRETARIO GENERALE**

E' copia conforme all'originale, in carta libera, per uso amministrativo.

Cairo Montenotte, li 31 maggio 2018

Visto:

L'Istruttore Direttivo
Liliana Dotto