



Comune di Cagnano Amiterno (Prov. L'Aquila)

Deliberazione della Giunta comunale

ORIGINALE

N. 44 Data 25/05/2018	Definizione degli obiettivi strategici in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali
--	---

L'anno duemiladiciotto il giorno venticinque del mese di maggio, alle ore 13:00, a seguito di regolari avvisi, la Giunta comunale si è riunita con la presenza dei signori:

<i>Iside DI MARTINO</i>	Sindaco	Presente
<i>Donatella TARQUINI</i>	V.Sindaco	Presente
<i>Emanuele CORAZZA</i>	Assessore	Assente

Fra gli assenti sono giustificati i signori: ===

Partecipa con funzioni consultive, referenti e di assistenza e ne cura la verbalizzazione (art. 97, c. 4.a, del T.U. n. 267/2000) il Segretario Comunale *DR.MARI ROBERTO*;

Il Sindaco, constatato che gli intervenuti sono in numero legale, dichiara aperta la riunione ed invita i convocati a deliberare sull'oggetto sopraindicato.

LA GIUNTA COMUNALE

Preso atto del d.Lg.vo 267/00;

Premesso che sulla proposta della presente deliberazione hanno espresso parere favorevole ai sensi dell'art 49 del decreto leg.vo 267/00:

- Il responsabile del servizio di ragioneria, per quanto concerne la regolarità contabile;
- ↷ Il responsabile del servizio interessato per quanto concerne la regolarità tecnica amm/va, hanno espresso parere favorevole ai sensi dell'art 49 del decreto leg.vo 267/00.

LA GIUNTA COMUNALE

PREMESSO:

- che la protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale è un diritto fondamentale. L'articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione europea («Carta») e l'articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea («TFUE») stabiliscono che ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano;

- che le persone fisiche devono avere il controllo dei dati personali che li riguardano e la certezza giuridica e operativa deve essere rafforzata tanto per le persone fisiche quanto per gli operatori economici e le autorità pubbliche tenuto conto che la rapidità dell'evoluzione tecnologica e la globalizzazione comportano nuove sfide per la protezione dei dati personali in considerazione, in particolare, di quanto segue:

- la portata della condivisione e della raccolta di dati personali è aumentata in modo significativo;
- la tecnologia attuale consente tanto alle imprese private quanto alle autorità pubbliche di utilizzare dati personali, come mai in precedenza, nello svolgimento delle loro attività. Sempre più spesso, le persone fisiche rendono disponibili al pubblico su scala mondiale informazioni personali che li riguardano;
- la tecnologia ha trasformato l'economia e le relazioni sociali e dovrebbe facilitare ancora di più la libera circolazione dei dati personali all'interno dell'Unione e il loro trasferimento verso paesi terzi e organizzazioni internazionali, garantendo al tempo stesso un elevato livello di protezione dei dati personali;

- Che tale evoluzione ha indotto l'Unione europea ad adottare il REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (di seguito solo GDPR);

- Che Il 24 maggio 2016 è entrato ufficialmente in vigore il Regolamento, che diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25 maggio 2018;

- Che con il GDPR è stato richiesto agli Stati membri un quadro più solido e coerente in materia di protezione dei dati, affiancato da efficaci misure di adeguamento, data l'importanza di creare il clima di fiducia funzionale allo sviluppo dell'economia digitale in tutto il mercato interno;

- che la Legge 25 ottobre 2017, n. 163 (art.13), ha delegato il Governo per l'adeguamento della normativa nazionale alle disposizioni del GDPR (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;

- che l'adeguamento al GDPR richiede di gestire, conformemente alle disposizioni dello stesso regolamento, il RISCHIO di violazione dei dati derivante dal trattamento e che, a tal fine, hanno preliminarmente individuati gli obiettivi strategici di tale adeguamento e, in particolare, gli obiettivi correlati alla gestione del rischio suddetto;

RILEVATO:

- che la gestione del rischio può essere efficacemente trattata secondo i principi e le linee guida contenute nella norma UNI ISO 31.000 secondo cui:
 - a) La gestione del rischio crea e protegge il valore. La gestione del rischio contribuisce in maniera dimostrabile al raggiungimento degli obiettivi ed al miglioramento della prestazione, per esempio in termini di salute e sicurezza delle persone, security, rispetto dei requisiti cogenti, consenso presso l'opinione pubblica, protezione dell'ambiente, qualità del prodotto gestione dei progetti, efficienza nelle operazioni, governance e reputazione.
 - b) La gestione del rischio è parte integrante di tutti i processi dell'organizzazione. La gestione del rischio non è un'attività indipendente, separata dalle attività e dai processi principali dell'organizzazione. La gestione del rischio fa parte delle responsabilità della direzione ed è parte integrante di tutti i processi dell'organizzazione, inclusi la pianificazione strategica e tutti i processi di gestione dei progetti e del cambiamento.
 - c) La gestione del rischio è parte del processo decisionale. La gestione del rischio aiuta i responsabili delle decisioni ad effettuare scelte consapevoli, determinare la scala di priorità delle azioni e distinguere tra linee di azione alternative.
 - d) La gestione del rischio tratta esplicitamente l'incertezza. La gestione del rischio tiene conto esplicitamente dell'incertezza, della natura di tale incertezza e di come può essere affrontata.
 - e) La gestione del rischio è sistematica, strutturata e tempestiva. Un approccio sistematico, tempestivo e strutturato alla gestione del rischio contribuisce all'efficienza ed a risultati coerenti, confrontabili ed affidabili.
 - f) La gestione del rischio si basa sulle migliori informazioni disponibili. Gli elementi in ingresso al processo per gestire il rischio si basano su fonti di informazione quali dati storici, esperienza, informazioni di ritorno dai portatori d'interesse, osservazioni, previsioni e parere di specialisti. Tuttavia, i responsabili delle decisioni dovrebbero informarsi, e tenerne conto, di qualsiasi limitazione dei dati o del modello utilizzati o delle possibilità di divergenza di opinione tra gli specialisti.
 - g) La gestione del rischio è "su misura". La gestione del rischio è in linea con il contesto esterno ed interno e con il profilo di rischio dell'organizzazione.
 - h) La gestione del rischio tiene conto dei fattori umani e culturali. Nell'ambito della gestione del rischio individua capacità, percezioni e aspettative delle persone esterne ed interne che possono facilitare o impedire il raggiungimento degli obiettivi dell'organizzazione.
 - i) La gestione del rischio è trasparente e inclusiva. Il coinvolgimento appropriato e tempestivo dei portatori d'interesse e, in particolare, dei responsabili delle decisioni, a tutti i livelli dell'organizzazione, assicura che la gestione del rischio rimanga pertinente ed aggiornata. Il coinvolgimento, inoltre, permette che i portatori d'interesse siano opportunamente rappresentati e che i loro punti di

vista siano presi in considerazione nel definire i criteri di rischio.

j) La gestione del rischio è dinamica. La gestione del rischio è sensibile e risponde al cambiamento continuamente. Ogni qual volta accadono eventi esterni ed interni, cambiano il contesto e la conoscenza, si attuano il monitoraggio ed il riesame, emergono nuovi rischi, alcuni rischi si modificano ed altri scompaiono.

k) La gestione del rischio favorisce il miglioramento continuo dell'organizzazione. Le organizzazioni dovrebbero sviluppare ed attuare strategie per migliorare la maturità della propria gestione del rischio insieme a tutti gli altri aspetti della propria organizzazione.

DATO ATTO, altresì, che la citata norma UNI ISO 31.000 contiene l'indicazione di predisporre e di attuare PIANI di trattamento del rischio e di documentare, secondo il principio di tracciabilità documentale, come le opzioni di trattamento individuate sono state attuate;

RITENUTO, pertanto, di includere, negli obiettivi strategici che il titolare intende perseguire per l'anno 2018 anche l'adozione di un apposito piano di protezione dei dati personali e di gestione del rischio di violazione

VISTO il parere favorevole espresso in ordine alla regolarità tecnica e contabile del presente atto (art. 49, 1° comma, D.Lgs. 267/2000);

DELIBERA

1) di definire, come di seguito riportati e in ragione di quanto sopra premesso, per nell'anno 2018, gli obiettivi strategici del intestato titolare in materia di protezione dei dati personali con riguardo al trattamento, al fine del loro recepimento e conseguente declinazione nei vari documenti di programmazione strategico-gestionale del titolare:

OBIETTIVO STRATEGICO n. 1

Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, mettere in atto, prioritariamente mediante informatizzazione del relativo processo gestionale, misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al GDPR, nel quadro di politiche adeguate in materia di protezione, istituendo e tenendo costantemente aggiornati i Registri delle attività e categorie di trattamento

OBIETTIVO STRATEGICO n. 2

Elaborare e attuare un Piano di protezione dei dati e di gestione del rischio di violazione (PPD) e documentare, secondo il principio di tracciabilità documentale, come le opzioni di trattamento individuate sono state attuate, integrando la protezione dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla protezione dei dati personali, secondo le disposizioni del GDPR nella gestione di tutti i processi del titolare, implementando la cultura della sicurezza nel contesto interno ed esterno dell'organizzazione, provvedendo, altresì, alla

designazione del Responsabile della Protezione dei Dati (RPD)

OBIETTIVO STRATEGICO n. 3

Garantire il processo di gestione del rischio di violazione dei dati personali, derivante dal trattamento, secondo i principi della norma UNI ISO 31000 e realizzare una politica di sicurezza dei dati personali partecipata e condivisa con gli interessati e gli stakeholder

OBIETTIVO STRATEGICO n. 4

Valutare la fattibilità dell'adesione ai codici di condotta di cui all'articolo 40 o a un meccanismo di certificazione di cui all'articolo 42 GDPR da utilizzare come elemento per dimostrare il rispetto degli obblighi del titolare del trattamento

OBIETTIVO STRATEGICO n. 5

Garantire la correlazione con il PTPC e gli altri strumenti di pianificazione, mediante inserimento degli obiettivi strategici in tema di protezione dei dati personali nei documenti di pianificazione del titolare

2) **di dare** mandato ai Responsabili degli Uffici comunali ogni atto gestionali conseguente la presente deliberazione,

3) **di dichiarare** il presente provvedimento immediatamente eseguibile, ai sensi dell'art. 134, comma 4, del d.lgs. 267/2000.

Il presente verbale viene sottoscritto come segue:

Il Segretario Comunale

(Dott. Roberto Mari)

Il Sindaco

(Iside Di Martino)

Il sottoscritto responsabile del servizio delle pubblicazioni aventi effetto di pubblicità legale, visti gli atti d'ufficio;

Visto lo statuto comunale,

ATTESTA

che la presente deliberazione è stata pubblicata, in data odierna, per rimanervi per 15 giorni consecutivi nel sito web istituzionale di questo Comune (PROT. ALBO N. 479) accessibile al pubblico (art. 32, comma 1, della legge 18 giugno 2009, n. 69) ed è stata compresa nell'elenco n. 2227 in data odierna, delle deliberazioni comunicate ai capigruppo consiliari (art. 125, del T.U. n. 267/2000).

Dalla residenza comunale, li 25/05/2015



Il Responsabile del servizio

Il sottoscritto, visti gli atti d'ufficio,

ATTESTA

che la presente deliberazione è stata pubblicata nel sito web istituzionale di questo Comune per quindici giorni consecutivi dal _____ al _____ ed è divenuta esecutiva oggi, decorsi 10 giorni dall'ultimo di pubblicazione (art. 134, c. 3, del T.U. n. 267/2000).

Che la presente deliberazione è immediatamente eseguibile (art. 134, comma 4, D.Leg.vo 18.08.2000 n. 267);

Dalla residenza comunale, li 25/05/2018

Il Segretario Comunale