



**CITTA' DI POTENZA
SEGRETERIA GENERALE**

OGGETTO: Regolamento UE n. 679/2016 – Linee guida per l'applicazione degli adempimenti in materia di trattamento dei dati personali delle persone fisiche.

Relazione istruttoria/illustrativa

PREMESSO CHE:

- La protezione dei dati personali è regolata, in Italia e in Europa, da un insieme articolato di norme di legge, tra cui spicca il Regolamento Europeo 2016/679 ("Regolamento").
- 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.
- Un individuo, che conferisce i propri dati personali, ha diritto di sapere in via preventiva come questi dati verranno trattati, nel rispetto di specifiche norme di legge, sia nel settore privato sia in quello pubblico. Spesso i termini *privacy* e "protezione dei dati personali" vengono utilizzati come sinonimi, ma hanno significato differente, posto che la *privacy* corrisponde alla riservatezza e al diritto alla propria vita privata e familiare, mentre la protezione dei dati personali afferisce al diritto da parte dell'individuo di avere il "controllo" sulle informazioni che lo riguardano. Tali principi sono considerati diritti fondamentali espressamente contemplati dalla Carta dei Diritti Fondamentali dell'Unione Europea, rispettivamente agli articoli 7 e 8.
- La più moderna ed aggiornata disciplina italiana, europea e internazionale, tutela gli individui ed obbliga i soggetti ai quali sono conferiti i dati personali (società, aziende, organizzazioni, enti pubblici, ecc.) ad utilizzarli lecitamente, per le finalità preventivamente dichiarate e strettamente necessarie al raggiungimento dello scopo per il quale gli stessi dati sono stati raccolti. In sostanza, l'individuo dovrebbe sapere preventivamente a chi sta fornendo i propri dati personali, per quale finalità e come tali dati saranno trattati. La finalità del trattamento dei dati personali, quindi, dovrebbe essere sempre chiara e



ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI

preventivamente dichiarata in modo trasparente all'utente. Questa impostazione vale a livello nazionale, europeo e internazionale (ad esempio, il trasferimento transfrontaliero dei dati a società dello stesso gruppo di una multinazionale).

- In Italia è vigente il Decreto Legislativo 30/6/2003, n. 196 "Codice in materia di protezione dei dati personali", come modificato dal D.Lgs. 10 agosto 2018, n. 101, entrato in vigore il 19/09/2018.
- Le principali novità che sono state introdotte dal Regolamento riguardano:
 - il diritto all'oblio;
 - il consenso (il regolamento definisce gli standard del consenso che è considerato una base residuale del trattamento ed è autonomo rispetto all'informativa);
 - un facile accesso ai propri dati personali da parte dell'interessato;
 - il diritto alla portabilità dei dati personali;
 - ridefinisce la figura del responsabile del trattamento precisandone la responsabilità;
 - l'utilizzo di un approccio *data protection by design e by default*;
 - l'introduzione dell'obbligo di nomina di un *Data Protection Officer* per enti pubblici ed aziende;
 - la responsabilità del titolare del trattamento per la conservazione della documentazione relativa alle modalità dei singoli trattamenti;
 - l'introduzione della DPIA (*Data Protection Impact Assessment*), cioè della valutazione preventiva dei rischi connessi con la *privacy*;
 - l'introduzione della *data breach notification*, ossia dell'obbligo a carico del responsabile del trattamento di notificare all'autorità di controllo la violazione dei dati personali entro 24 ore dal momento in cui ne è venuto a conoscenza;
 - l'istituzione della consultazione preventiva dell'autorità di controllo;
 - l'istituzione dell'*European Data Protection Board*, che avrà un ruolo primario soprattutto nelle vicende di carattere transfrontaliero che riguardano il trasferimento dei dati tra soggetti della UE;
 - le sanzioni, che possono arrivare sino alla maggior somma tra 20.000.000 di euro o il 4% del fatturato annuo;
 - il superamento dell'obbligo di notifica al Garante.



ORIGINALE
IL SEGRETARIO GENERALE
Carlo GERARDI

RILEVATO CHE

- Vanno adottate misure di sicurezza adeguate che riducano al minimo il rischio di violazione/perdita di dati e/o di informazioni e/o illecite diffusioni o comunicazioni a terzi.
- Tutto ciò che si presenta come un rischio per la sicurezza lo è anche per la *privacy* e, quindi, è necessario preventivamente valutare i rischi (mediante audit ed elaborazione di DPIA) e così prevenire eventuali perdite di dati.
- Il titolare del trattamento deve identificare i flussi di dati personali relativi a ogni trattamento e mantenerli aggiornati in un inventario dei trattamenti di dati personali, in linea con quanto prescritto dall'art.30 del Regolamento.
- Il titolare o responsabile del trattamento deve identificare, definire e documentare le basi legali per il trattamento dei dati personali individuati.
- Il titolare o responsabile del trattamento deve individuare e attuare le misure di sicurezza dei dati personali relative alla protezione dei dati personali e mantenere attive e aggiornate quelle già adottate in precedenza anche seguendo quanto emerso dall'ambito della "Protezione dei dati personali *by design* e *by default*".
- Il titolare o responsabile deve stabilire un processo documentato di gestione degli incidenti relativi alla protezione dei dati personali, in ambito ICT, che includa:
 - la valutazione e la gestione delle violazioni dei dati personali e procedure per mitigare il danno causato da tali violazioni;
 - le modalità di notifica alle autorità di controllo (entro 72 ore dalla presa di conoscenza della violazione), nel caso l'organizzazione sia titolare del trattamento, di ogni violazione dei dati personali che potrebbe causare un rischio per i diritti e la libertà delle persone fisiche.
- Il titolare o responsabile del trattamento deve stabilire un processo per un semplice e tempestivo accesso ai diritti degli interessati.
- Il paragrafo 1 dell'art. 32 del Regolamento richiede che "Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e la libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio". Questo richiede che venga svolta l'analisi dei rischi che



ORIGINALE
IL SEGRETARIO GENERALE
Gianluca GERARDI

insistono sui sistemi utilizzati per il trattamento dei dati, al fine di garantire riservatezza, integrità e disponibilità.

- L'identificazione dei rischi e la conseguente mappatura è preliminare all'analisi dei rischi del trattamento di dati personali e andrebbe effettuata su più livelli (art. 35 GDPR).
- Tenendo conto dello stato dell'arte e dei costi di adeguamento, nonché della natura, dell'oggetto, 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, il titolare e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:
 - la pseudonimizzazione e la cifratura dei dati personali;
 - la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
 - la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
 - una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.
- Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati.
- Il titolare o il responsabile del trattamento fanno sì che, chiunque agisca sotto la loro autorità e abbia accesso a dati personali, non tratti tali dati, se non è istruito in tal senso, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
- Dato atto, altresì, che la norma UNI ISO 31000 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 dell'Ente, che il titolare intende perseguire per l'anno 2019, anche l'adozione di un apposito piano di protezione dei dati personali e di gestione del rischio di violazione degli stessi.

Visto il parere tecnico favorevole espresso ai sensi dell'art. 49 del D. Lgs n. 267/2000;



ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI

Dato atto che il presente atto non comporta alcuna variazione, ai fini contabili, in termini di spesa o di entrata;

Si propone l'adozione della seguente deliberazione di competenza della Giunta Comunale

1) Di stabilire, come di seguito riportati e in ragione di quanto sopra premesso, per l'anno 2019, gli obiettivi strategici della presente organizzazione, in qualità di titolare del trattamento dati personali, al fine del loro recepimento e conseguente declinazione nei vari documenti di programmazione strategico-gestionale dell'Ente:

a. I dirigenti devono individuare , con provvedimento espresso, e assicurare la costante continuità delle seguenti figure:

- gli autorizzati al trattamento dei dati personali, ciascuno in relazione ai procedimenti amministrativi singolarmente assegnati che contengono esclusivamente il trattamento dei dati, così come richiesto dal d.lgs. 101/2018 Art. 2-quaterdecies . Le designazioni devono comprendere l'elenco completo dei trattamenti, in relazione ai trattamenti indicati nel relativo registro, da aggiungersi costantemente in caso di variazioni, unitamente alle designazioni del personale
- uno o più "referenti *privacy*" per ciascuna direzione, con il compito di supportare gli autorizzati al trattamento dei dati personali, sia a livello informativo che operativo.

Devono, altresì, provvedere alla valutazione d'impatto sulla protezione dei dati personali, consultando il DPO come previsto dall'art. 35 Del Regolamento UE 679/2016 e tenuto conto del provvedimento del Garante per la protezione dei dati personali [doc. web n. 9058979]

Devono, rendere, inoltre, disponibili agli interessati specifiche informative, secondo gli art. 13 e art. 14 del Regolamento UE 679/2016, sul trattamento dei dati personali costantemente aggiornate e facilmente accessibili, redatte con la collaborazione del Data Protection Officer.

b. Istituire, a cura del Segretario Generale, lo *staff* del *Data Protection Officer*, presieduto dal DPO stesso e composto dal Referente interno della *privacy* dell'Ente, dipendente comunale di categoria D, nominato dal Segretario Generale, competente in materia di *governance* e gestione della protezione dei dati personali , e dai "referenti *privacy*", designati dai dirigenti . Lo *staff* dovrà adempiere ai seguenti compiti:

- redigere il Regolamento sulla protezione dei dati personali, in conformità con la normativa europea e nazionale;
- curare la comunicazione interna ed esterna relativa alle tematiche della *privacy*;



ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI

- monitorare il rispetto delle politiche in materia di protezione dei dati personali, attraverso questionari di autovalutazione, attività di *audit* interno, o con riguardo alla gestione di reclami, richieste o possibili violazioni;
- svolgere attività di *front-end* per ogni reclamo diretto alla propria direzione o settore;
- predisporre il "Registro delle attività di trattamento e delle misure di sicurezza adottate per la corretta gestione delle banche dati comunali e valutazione di impatto sulla protezione dei dati" in linea con quanto prescritto dall'art.30 del Regolamento UE 679/2016, da sottoporre all'approvazione da parte della Giunta Comunale. La compilazione e l'aggiornamento periodico delle schede del Registro dovranno avvenire almeno una volta all'anno da parte dei referenti *privacy*, a cui i dati afferiscono per le parti di propria competenza, coordinati dal Referente interno unitamente al DPO;
- svolgere ogni altro compito assegnato dal DPO.

c. Affidare al *Data Protection Officer* :

- la redazione e l'attuazione di un piano di formazione per il personale interno in materia di protezione dei dati personali secondo gli art. 29 e 32 del Regolamento UE;
- la redazione e l'attuazione di un piano di protezione dei dati e di gestione del rischio di violazione (PRG), secondo le disposizioni del GDPR, provvedendo, altresì, a definire le procedure per la gestione dei reclami, quelle di risposta agli incidenti di sicurezza, nonché la tipologia di comunicazione da trasmettere, in caso di *data breach*, ai soggetti interessati e all'Autorità;
- la redazione di informative per il personale riguardanti le politiche organizzative in materia di *privacy*, procedure o prassi adottate/da adottarsi, anche aggiornando e rendendo accessibili le informazioni per gli utenti;
- la trasmissione agli incaricati *privacy* di processi documentati per la valutazione dei rischi sulla protezione dei dati personali (DPIA), in relazione all'utilizzo di nuovi prodotti, tecnologie o servizi;
- la consulenza ai dirigenti in merito alla valutazione d'impatto sulla protezione dei dati e la relativa sorveglianza sullo svolgimento della stessa.

2) Prevedere adeguate risorse finanziarie destinate al raggiungimento dei suddetti obiettivi;

3) Stabilire l'inserimento degli obiettivi, approvati col presente atto, nei documenti di programmazione dell'Ente;

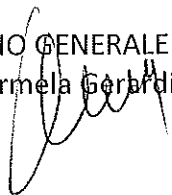


ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI

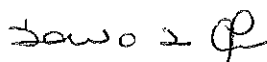
4) Dare atto che Il sindaco delega ciascun dirigente a svolgere le funzioni monocratiche con potere di firma per qualsiasi atto di designazione relativo alla materia di gestione della protezione dei dati personali , ognuno per la propria competenza .

5) Dichiarare, con successiva e separata votazione favorevole, unanime e palese, la presente deliberazione immediatamente eseguibile, ai sensi e per gli effetti di cui all'art. 134, comma 4, del D. Lgs 18.08.2000 n. 267, stante l'urgenza di dare seguito al presente provvedimento.

IL SEGRETARIO GENERALE
Dott.ssa Carmela Gerardi



IL SINDACO
Ing. Dario De Luca



ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI



OGGETTO: Regolamento UE n. 679/2016 – Linee guida per l'applicazione degli adempimenti in materia di trattamento dei dati personali delle persone fisiche.

Sulla presente proposta, in ordine alla regolarità tecnica ai sensi dell'art. 49, comma 1, del decreto legislativo 18 agosto 2000, n. 267 (T.U. Enti Locali), si esprime il seguente parere:

favorevole.

Potenza, 28-2-2019

IL SEGRETARIO GENERALE
Dott.ssa Carmela Gerardi



ORIGINALE
IL SEGRETARIO GENERALE
Carmela GERARDI