

COMUNE DI RIALTO

PROVINCIA DI SAVONA

DELIBERAZIONE DELLA GIUNTA COMUNALE

N° 22 DEL 21.05.2018

OGGETTO: REGOLAMENTO EUROPEO PRIVACY UE/2016/679 - GENERAL DATA PROTECTION REGULATION (GDPR). ATTO DI INDIRIZZO.

L'anno DUEMILADICIOTTO addì VENTUNO del mese di MAGGIO alle ore 18,00 nella sede Comunale.

Previo esaurimento delle formalità di rito sono stati convocati i componenti di questa Giunta Comunale.

Risultano:

Nome e Cognome	Presente	Assente
CASANOVA Silvio Sindaco	X	
BRUNET Michela Vice-Sindaco		X
ULTRA Lorenzo Assessore	X	
TOTALI	2	1

Assiste il Segretario Comunale Dott. Silvano FERRANDO.

Il Signor CASANOVA Silvio – Sindaco, assunta la presidenza e constatata la legalità dell'adunanza dichiara aperta la seduta e pone in discussione la seguente pratica segnata all'ordine del giorno:

OGGETTO: REGOLAMENTO EUROPEO PRIVACY UE/2016/679 - GENERAL DATA PROTECTION REGULATION (GDPR). ATTO DI INDIRIZZO.

LA GIUNTA COMUNALE

VISTO il Codice dell'Amministrazione Digitale, D.Lgs. n. 82/2005, così come modificato dal D.Lgs. n. 179/2016, che all'art. 51, rubricato "Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", prevede che "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta";

PRESO ATTO che con Circolare del 18 aprile 2017, n. 2/2017, pubblicata in G.U. Serie Generale n. 103 del 5.05.2017, l'Agenzia per l'Italia Digitale (AGID), al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi delle Pubbliche Amministrazioni, ha disposto la sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" con nuove misure minime per la sicurezza informatica a cui le stesse Pubbliche Amministrazioni sono tenute a conformarsi entro il termine del 31.12.2017;

CONSIDERATO che il 25 maggio 2016 è entrato in vigore il Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

RILEVATO che il summenzionato Regolamento è direttamente applicabile in ciascuno degli Stati membri dell'Unione Europea ed entrerà in vigore il 25 maggio 2018;

CONSIDERATO che con il Regolamento Europeo Privacy UE/2016/679 viene recepito nel nostro ordinamento giuridico il "principio di accountability" (obbligo di rendicontazione) che impone alle Pubbliche Amministrazioni titolari del trattamento dei dati:

- di dimostrare di avere adottato 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, 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;
- che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento, prevedendo, altresì, l'obbligo del titolare o del responsabile del trattamento della tenuta di apposito registro delle attività di trattamento, compresa la descrizione circa l'efficacia delle misure di sicurezza adottate;
- che il registro di cui al punto precedente, da tenersi in forma scritta o anche in formato

elettronico, deve contenere una descrizione generale delle misure di sicurezza tecniche e organizzative e che su richiesta, il titolare del trattamento o il responsabile del trattamento sono tenuti a mettere il registro a disposizione dell'autorità di controllo;

TENUTO CONTO, inoltre, che il Regolamento Europeo Privacy UE/2016/679 ha:

- reintrodotta l'obbligatorietà della redazione del documento programmatico sulla sicurezza (**DPS**), obbligo previsto dal D.Lgs. 196/2003 e abrogato dal Decreto Legge n. 5 del 9 febbraio 2012, convertito dalla legge n. 35 del 4 aprile 2012;
- disciplinato la nuova figura del "Data Protection Officer" (**DPO**), responsabile della protezione dei dati personali che le pubbliche amministrazioni hanno l'obbligo di nominare e deve sempre essere "coinvolto in tutte le questioni riguardanti la protezione dei dati personali";
- rafforzato i poteri delle Autorità Garanti nazionali ed inasprito le sanzioni amministrative a carico di imprese e pubbliche amministrazioni, in particolare, in caso di violazioni dei principi e disposizioni del Regolamento, le sanzioni possono arrivare fino a 10 milioni di euro o per le imprese fino al 2% - 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore;

DATO ATTO che la nuova normativa europea fa carico alle Pubbliche Amministrazioni di non limitarsi alla semplice osservanza di un mero adempimento formale in materia di privacy, conservazione e sicurezza dei dati personali, ma attua un profondo mutamento culturale con un rilevante impatto organizzativo da parte dell'Ente nell'ottica di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie (cloud computing, digitalizzazione, social media, cooperazione applicativa, interconnessione di banche dati, pubblicazione automatizzata di dati on line) nelle amministrazioni pubbliche;

RITENUTO, pertanto, necessario realizzare un "modello organizzativo" da implementare in base ad una preliminare analisi dei rischi e ad un'autovalutazione finalizzata all'adozione delle migliori strategie volte a presidiare i trattamenti di dati effettuati, abbandonando l'approccio meramente formale del D.Lgs. 196/2003, limitato alla mera adozione di una lista "minima" di misure di sicurezza, realizzando, piuttosto, un sistema organizzativo caratterizzato da un'attenzione multidisciplinare alle specificità della struttura e della tipologia di trattamento, sia dal punto di vista della sicurezza informatica e in conformità agli obblighi legali, sia in considerazione del modello di archiviazione e gestione dei dati trattati.

RITENUTO, altresì, necessario prevedere, al contempo, non solo l'introduzione di nuove figure soggettive e professionali che dovranno presidiare i processi organizzativi interni per garantire un corretto trattamento dei dati personali, tra cui la figura del Responsabile della Protezione dei dati personali (DPO), ma altresì l'adozione di nuove misure tecniche ed organizzative volte a garantire l'integrità e la riservatezza dei dati, la disponibilità e la resilienza dei sistemi e dei servizi di

trattamento, la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico, nonché la verifica e la valutazione dell'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento;

RILEVATO che ai sensi dell'art. 37 c. 5 e 6 del Regolamento Europeo Privacy UE/2016/679 il Responsabile della protezione dei dati, chiamato a dare attuazione agli obblighi imposti dalla suindicata normativa, è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39 e può essere un dipendente del soggetto titolare del trattamento o del responsabile del trattamento **oppure assolvere i suoi compiti in base a un contratto di servizi;**

DATO ATTO che all'interno del personale dipendente dell'Ente non sono presenti professionalità dotate delle conoscenze specialistiche, che presentano rilevanti aspetti di natura informatica, richieste dall'art. 37 c. 5 del Regolamento Europeo Privacy UE/2016/679 e necessarie allo svolgimento delle funzioni previste dal successivo art. 39, tra le quali figurano la mappatura dei procedimenti amministrativi, l'analisi della conformità del trattamento al GDPR, la valutazione del rischio, la redazione del registro trattamenti, la valutazione dell'impatto, la formazione del personale, la nomina DPO ed RTD, la compilazione dell'allegato 2 circolare Agid 2/17 ;

CONSIDERATA la necessità di ottemperare agli obblighi imposti dal Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation) che stabilisce le nuove norme in materia di protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché le norme relative alla libera circolazione di tali dati;

RITENUTO, pertanto, di formulare atto di indirizzo al Responsabile del Servizio Finanziario a provvedere all'individuazione, mediante appalto di servizi sul Mercato Elettronico della Pubblica Amministrazione (M.E.P.A.), conformemente a quanto previsto dall'art. 37 c. 6 del Regolamento Europeo Privacy UE/2016/679, di un operatore economico in possesso dei requisiti necessari a garantire l'assolvimento dei suindicati obblighi;

ACQUISITI i pareri favorevoli in ordine alla regolarità tecnica e contabile dei Responsabili dei Servizi competenti, ai sensi dell'art. 49 del D. lgs. N. 267/2000;

Con votazione unanime, espressa nelle forme di legge

DELIBERA

1. Tutto quanto in premessa costituisce parte integrante e sostanziale della presente
2. **DI DARE ATTO** che all'interno del personale dipendente dell'Ente non sono presenti professionalità dotate delle conoscenze specialistiche, che presentano rilevanti aspetti di natura informatica, richieste dall'art. 37 c. 5 del Regolamento Europeo Privacy UE/2016/679 e necessarie allo svolgimento delle funzioni previste dal successivo art. 39, tra le quali figurano la mappatura dei procedimenti amministrativi, l'analisi della conformità del trattamento al GDPR, la valutazione del rischio, la redazione del registro trattamenti, la valutazione dell'impatto, la formazione del personale, la nomina DPO ed RTD, la compilazione dell' allegato 2 circolare Agid 2/17;
3. **DI FORMULARE** atto di indirizzo al Responsabile dell'Area Finanziaria a provvedere all'individuazione, mediante appalto di servizi sul Mercato Elettronico della Pubblica Amministrazione (M.E.P.A.), conformemente a quanto previsto dall'art. 37 c. 6 del Regolamento Europeo Privacy UE/2016/679, di un operatore economico in possesso dei requisiti necessari a garantire l'assolvimento dei suindicati obblighi imposti dal Regolamento Europeo Privacy UE/2016/679 o GDPR (General Data Protection Regulation);
4. **DI DISPORRE** la pubblicazione della presente sull'Albo Pretorio on line del Comune ;
5. **DI DICHIARARE**, con successiva unanime votazione, stante l'urgenza del provvedere, la presente immediatamente esecutiva, ai sensi dell'art. 134 c. 4 del D.lgs. n° 267/2000;

IL PRESIDENTE
f.to (Silvio Casanova)

IL SEGRETARIO COMUNALE
f.to (Dott. Silvano FERRANDO)

Pareri resi ai sensi dell'art. 49 comma 1 T.U. 267/2000.

REGOLARITA' TECNICA

In ordine alla regolarità tecnica del presente provvedimento è stato espresso, in data 21.05.2018 parere **FAVOREVOLE**, per quanto di competenza.

IL RESPONSABILE DEL SERVIZIO
f.to (Silvio Casanova)

REGOLARITA' CONTABILE

In ordine alla regolarità contabile del presente provvedimento è stato espresso, in data 21.05.2018 parere **FAVOREVOLE**, per quanto di competenza.

IL RESPONSABILE DEL SERVIZIO FINANZIARIO
f.to (Silvio CASANOVA)

CERTIFICATO DI PUBBLICAZIONE

Il sottoscritto Messo Comunale certifica che il presente verbale viene affisso all'Albo Pretorio di questo Comune per 15 giorni consecutivi dal

Rialto, li 13.06.2018

IL MESSO COMUNALE
f.to (Rag. Luca Canepa)

CERTIFICATO DI ESECUTIVITA'

La presente è divenuta esecutiva il

IL SEGRETARIO COMUNALE
(Dott. Silvano Ferrando)