Comune di Striano

Città Metropolitana di Napoli

Servizio AA.GG.

CONFERIMENTO DELL'INCARICO PER L'ATTUAZIONE DEL REGOLAMENTO U.E n. 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI E INDIVIDUAZIONE RESPONSABILE PROTEZIONE DATI (RPD) - **Disciplinare tecnico.**

1. Indicazioni generali

Il Regolamento Generale sulla Protezione dei dati personali (Regolamento UE 679/2016 detto anche "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, pubblicato sulla G.U.U.E. il 4.5.2016, diventerà definitivamente applicabile in via diretta in tutti i Paesi UE a partire dal 25.5.2018.

Le disposizioni contenute nel nuovo Regolamento europeo per la protezione dei dati personali impongono alle Pubbliche Amministrazioni di assicurare, l'applicazione tassativa della ~~normativa europea sul trattamento dei~~ dati, la cui responsabilità ultima cade sul titolare del trattamento, figura che negli enti locali è ricoperta dal Sindaco.

L'adozione delle disposizioni contenute nel Regolamento europeo incide notevolmente sull'organizzazione interna e richiederà la ricognizione, la valutazione e l'eventuale adeguamento delle misure di sicurezza normative, organizzative e tecnologiche, già adottate dagli enti a tutela della privacy. Il modello immaginato dal legislatore Europeo ripercorre la strada già tracciata dalle norme in materia di sicurezza del lavoro, e passa attraverso le seguenti fasi:

- un'analisi del contesto, con la mappatura dei processi soggetti a rischio, e rilevazione dei livelli di sicurezza oggi esistenti, sia dal punto di vista informatico, che da quello analogico;
- la definizione e pianificazione delle misure necessarie al raggiungimento di un adeguato livello di sicurezza, conforme agli standards previsti;
- l'implementazione di un sistema di "autocontrollo", che preveda il continuo monitoraggio, l'aggiornamento e l'implementazione delle misure di sicurezza, e la documentazione di tutta l'attività che viene svolta a tali fini;
- la formazione periodica degli operatori dei diversi settori interessati, al fine di accrescere la consapevolezza dei rischi ed aumentare la capacità di prevenzione.
- l'individuazione e nomina del RPD (Responsabile Protezione Dati)

L'adeguamento alle nuove norme costituisce un'occasione di riflessione sull'organizzazione dell'ente e sul livello di sicurezza del trattamento dei dati attualmente in essere, al fine di apportare i correttivi e i miglioramenti necessari. Sono richieste, pertanto, le seguenti competenze:

-comprovate competenze giuridiche, con particolare riguardo al diritto amministrativo, alla legislazione degli enti locali e alle norme sulla tutela dei dati personali.

- comprovate competenze informatiche, con particolare riguardo alla gestione di sistemi informativi complessi, afferenti alla gestione di servizi pubblici o privati comportanti il trattamento di dati personali.

È richiesto, pertanto, per l'accesso alla procedura, diploma di laurea in ingegneria oppure in giurisprudenza/economia e commercio o lauree equipollenti (per tutte corso magistrale, laurea specialistica o

vecchio ordinamento); inoltre, documentata esperienza lavorativa maturata presso aziende private, enti locali o altre pubbliche amministrazioni, in qualità di dipendenti, consulenti o collaboratori nel settore di interesse (i candidati devono essere in possesso di idonea specializzazione nella materia della privacy risultante da titoli accademici e/o dall'attività ed esperienza maturata desumibile dal curriculum presentato).

La valutazione dei titoli indicati nel curriculum assume valore prevalente rispetto all'offerta economica ed è determinante ai fini dell'affidamento dell'incarico.

2. Organizzazione amministrativa dell'ente:

L'ente è organizzato in 5 Servizi: Affari Generali, Finanziario, Urbanistica, Lavori Pubblici e Polizia Locale, a capo dei quali sono posti n. 4 responsabili di servizio, di cui n. 1 ad interim. L'ente è dotato di un istruttore Centro Elaborazione Dati (Ced).

3. Ubicazione fisica degli uffici e servizi

Gli uffici e i servizi dell'ente sono dislocati nella struttura centrale e in una periferica dove sono situati i Servizi Sociali.

4. Trattamenti di dati

Ciascuno degli uffici e servizi svolge attività e compiti che comportano il trattamento di dati personali di cittadini, utenti, contribuenti, fornitori, dipendenti. In alcuni casi, vengono trattati anche dati sensibili. Il trattamento viene effettuato per lo più con modalità informatizzate, con specifici programmi gestionali in rete, ma è presente anche un archivio cartaceo.

I trattamenti più importanti e significativi vengono effettuati a prescindere dal consenso degli interessati per l'esercizio di funzioni istituzionali o previste per legge: anagrafe, stato civile, elettorale, leva militare, statistica e censimenti; tributi; edilizia e urbanistica, raccolta rifiuti.

Altri trattamenti avvengono su base volontaria, in relazione alla richiesta di determinati servizi da parte dei cittadini/utenti: servizi scolastici, servizi sociali, servizi culturali e turistici, servizi finanziari, da cui emergono talvolta anche dati sensibili.

Altri ancora sono connessi alla necessità di utilizzare determinate procedure previste per legge, che richiedono il trattamento di dati sensibili o giudiziari (es: gare di appalto).

Infine, vengono trattati i dati del proprio personale dipendente, comprendenti anche dati sensibili.

5. Organizzazione informatica

Il sistema informatico comunale consta di un quarantina di computer con sistemi operativi Microsoft, distribuiti sui vari uffici comunali.

Nella sede centrale si trovano la maggior parte dei computer, collegati in rete per mezzo di switch dislocati su 3 piani differenti, che confluiscono tutti nell'Armadio Rack posto nella sala CED, servita da Fibra ottica.

In tale armadio è presente, inoltre, un firewall, che oltre a fungere da protezione (attraverso impostazione delle regole), serve anche per il NAT della Rete, disponendo il comune di soli 5 indirizzi IP pubblici.

La sede di Via B. Marciano, dove sono dislocati i Servizi Sociali, è collegata attraverso una linea indipendente, ma può condividere risorse e dati con la sede centrale grazie all'utilizzo di un sistema di Cloud Computing.

Sala macchine - Nella sala CED, dotata di porta blindata in ferro, sono ospitati i server comunali, alcuni fisici ed un altro virtualizzato, quest'ultimo installato su un sistema clustering vmware.

I server fisici hanno le seguenti utilità:

N.° 1 Server fisico che ospita gli applicativi Halley/Alphasoft. Sistema Operativo Linux / CENTOS (Demografici, Polizia Municipale)

N° 1 Server fisico che ospita gli applicativi Publisys (Protocollo, Tributi, Finanziario, Uffici Tecnici, SUAP, Atti Amministrativi etc.).

N.° 1 Server fisico per l'utilizzo di Antivirus centralizzato. Sistema Operativo Windows 2012

N° 1 Server fisico per che ospita web application open source per Amminitrsazione Trasparente, AVCP xml, Gestione Segnalazioni, Intranet (realizzati da personale interno). Sistema Operativo Ubuntu Server + LAMP.

N° 1 Server fisico per prove e back-up temporanei.

N° 1 NAS interno (un altro è posto all'esterno) per il back-up dei dati degli applicativi comunali

Due servizi sono esternalizzati: il sito internet attualmente in hosting presso la ditta ARUBA SpA e il servizio email gestito dalla stessa azienda.

Il palazzo comunale è dotato di un sistema di videosorveglianza a presidio degli accessi; alcune telecamere sono altresì installate sul territorio comunale, per il controllo del territorio e la prevenzione di illeciti. Il ced "ospita" un server per la videosorveglianza, al quale gli addetti del Ced non hanno accesso, potendo verificare solo lo stato di accensione. L'accesso ai dati registrati dal sistema di videosorveglianza è disciplinata da apposito regolamento.

6. Oggetto dell'incarico

Le attività che l'Ente intende affidare all'esterno, nell'ambito dell'incarico di prestazione di servizi e sulla base delle quali dovrà essere formalizzata l'offerta, sono le seguenti:

- **a.** nomina del RDP per il periodo di due anni:
- **b.** supporto e assistenza alla mappatura dei processi, per individuare quelli collegati al trattamento dei dati personali;
- **c.** individuazione, tra i processi risultanti dalla mappatura, di quelli che presentano rischi, con una prima valutazione degli stessi i termini di maggiore o minore gravità;
- **d.** supporto e assistenza alla mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento;
- **e.** elaborazione del piano di adeguamento complessivo, contenente le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi (se necessario) e dei tempi previsti, nonché delle attività di monitoraggio;
- **f.** interventi formativi del personale;
- **g.** predisposizione e supporto alla compilazione ed aggiornamento del registro dei trattamenti di dati personali e del registro delle categorie di attività;
- **h.** proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni.
- **i.** Valutazione di impatto sulla protezione dei dati.

7. Contenuti e tempistica

7.1. Nomina del RDP

La nomina del RDP avrà decorrenza dalla data di conferimento dell'incarico e durata triennale.

L'istituzione della nuova figura del *Responsabile della protezione dei dati* (in seguito indicato con 'RPD') è la principale novità normativa del Regolamento europeo, che mira al potenziamento del controllo dell'efficacia e della sicurezza dei sistemi di protezione dei dati personali.

Il Responsabile della protezione dei dati è incaricato dei seguenti compiti:
a) informare e fornire consulenza al Titolare e al Responsabile, nonché ai dipendenti che eseguono il trattamento, in merito agli obblighi derivanti dal RGPD e dalle altre normative relative alla protezione dei dati. A tal fine, il RPD deve indicare al Titolare e/o al Responsabile 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, ferme 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 parere in merito alla valutazione di impatto sulla protezione dei dati (DPIA), fornire gli opportuni suggerimenti per lo svolgimento delle attività nel modo più sicuro e meno impattante, sorvegliarne lo svolgimento;

e) cooperare con il Garante per la protezione dei dati personali e fungere da punto di contatto per detta Autorità;

f) provvedere alla corretta tenuta dei registri del Titolare e del/dei Responsabili sul trattamento.

g) supportare il Titolare e i Responsabili del trattamento nell'individuare processi organizzativi idonei a contemperare le esigenze della gestione delle attività di competenza e le esigenze di tutela dei dati;

7.2; 7.3; 7.4 - Mappatura dei processi, individuazione dei rischi e mappatura degli incarichi

L'attività di mappatura dei processi, degli incaricati e l'individuazione del livello di protezione o di rischio sono il punto di avvio del procedimento e definiscono l'iter per raggiungere gli obiettivi previsti dal legislatore europeo.

L'indagine dovrà, quindi, essere svolta in maniera accurata, settore per settore, sulla base di check list fornite dai professionisti incaricati; i responsabili dei singoli servizi, nonché l'addetto al Centro elaborazione dati forniranno il supporto necessario e tutte le informazioni richieste, acquisendole a loro volta dai fornitori esterni, qualora non siano a disposizione dell'ente.

Le surriferite attività devono concludersi entro 15 giorni naturali e consecutivi dal conferimento dell'incarico.

7.5. Elaborazione del piano di adeguamento

Il piano di adeguamento contiene le proposte di miglioramento del livello di sicurezza per i processi che presentano rischi, con stima dei costi, se necessario, e dei tempi previsti, nonché delle attività di monitoraggio e le tempistiche.

Le misure tecniche e 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, altresì, misure tecniche e organizzative: i sistemi di autenticazione; i sistemi di autorizzazione; sistemi di protezione (antivirus; firewall; antintrusione; altro); le misure antincendio; i sistemi di rilevazione di intrusione; i 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.*

Il piano dovrà essere presentato al responsabile del procedimento entro 20 giorni naturali e consecutivi dalla scadenza del termine di cui al punto precedente; entro 10 giorni naturali e consecutivi devono essere apportate le eventuali modifiche e integrazioni concordate, e consegnata la relazione definitiva.

7.6. Interventi formativi del personale

Gli interventi formativi del personale devono prevedere una formazione di base, da impartire a tutti i dipendenti, e una formazione specialistica per i dipendenti che svolgono attività classificate a rischio più elevato. Il piano di formazione dovrà essere presentato in contemporanea al piano di adeguamento di cui al punto 5, e dovrà essere programmato in modo da fare fronte alle carenze riscontrate nell'ambito della mappatura. Il calendario e le modalità di articolazione della formazione saranno concordati con il Titolare del trattamento o suo delegato, e/o, in caso di formazione riguardante specifici settori, con il responsabile competente.

7.7. Predisposizione, supporto alla compilazione, aggiornamento e tenuta del registro dei trattamenti di dati personali e del registro delle categorie di attività

Il Registro delle attività di trattamento dovrà prevedere almeno le seguenti informazioni:

a. il nome e i dati di contatto del Comune, eventualmente del Contitolare del trattamento, del RPD;

b. le finalità del trattamento;

c. la sintetica descrizione delle categorie di interessati (cittadini, residenti, utenti, dipendenti, amministratori, parti, altro), nonché le categorie di dati personali (dati identificativi, dati genetici, dati biometrici, dati relativi alla salute);

d. le categorie di destinatari a cui i dati personali sono stati o saranno comunicati: persona fisica o giuridica; autorità pubblica; altro organismo destinatario;

e. l'eventuale trasferimento di dati personali verso un paese terzo od 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 e organizzative del trattamento adottate.

h. Registro delle categorie di attività

Il Registro delle categorie di attività trattate da ciascun Responsabile del trattamento dovrà prevedere le seguenti informazioni:

a. il nome e 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;

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

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

La predisposizione dei registri sarà a cura del RDP, non appena conclusa la fase di mappatura prevista al punto 2.

La tenuta, il supporto alla compilazione e l'aggiornamento dei registri sarà a cura del RDP che dovrà provvedervi tempestivamente coordinandosi e supportando i responsabili del trattamento; con cadenza semestrale i registri dovranno essere sottoposti al controllo e alla vidimazione, rispettivamente: registro dei trattamenti - titolare del trattamento o suo delegato; registro delle categorie di attività trattate - responsabili dei servizi competenti.

7.8. proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni. La proposta di adeguamento della modulistica in uso agli uffici, se non conforme alle nuove disposizioni, dovrà essere completata entro due mesi dalla data di scadenza dei termini per la mappatura di cui al punto 2.

7.9. Valutazione di 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 Titolare, su segnalazione del Responsabile del trattamento, prima di effettuare il trattamento, deve effettuare una valutazione dell'impatto del medesimo trattamento ai sensi dell'art. 35, RGDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Il Titolare si avvale della consulenza tecnica del RDP, il quale, entro 15 giorni dalla richiesta, dovrà descrivere il trattamento, valutarne necessità e proporzionalità, individuare le migliori modalità di gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali e permette di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

8. Inadempimento e ritardo – penalità

Il ritardo nell'esecuzione delle prestazioni indicate ai paragrafi 7.2, 7,3, 7,4, 7.5 e nella predisposizione dei registri previsti dal 7.7 comporterà l'applicazione di una penale giornaliera di € 100,00 per ogni giorno lavorativo di ritardo.

Il ritardo nell'esecuzione delle altre prestazioni previste dal capitolato comporterà l'applicazione di una penale giornaliera di € 50,00 per ogni giorno lavorativo di ritardo.

In ogni caso, qualora il ritardo superi i 15 giorni, si farà luogo alla risoluzione del contratto, ai sensi degli artt. 1453 e 1454 del codice civile, con richiesta di risarcimento dei danni.

L'applicazione della penale sarà preceduta da formale contestazione scritta; l'aggiudicatario avrà la facoltà di presentare le proprie contro-deduzioni nel termine indicato nella contestazione, non inferiore a 10 giorni dalla data del ricevimento della contestazione stessa.

Qualora entro il termine stabilito l'aggiudicatario non fornisca alcuna motivata giustificazione scritta, ovvero qualora le stesse non fossero ritenute accoglibili, il Comune applicherà le penali previste, motivando adeguatamente in ordine al mancato accoglimento delle giustificazioni.

Non è comunque precluso al Comune il diritto di sanzionare eventuali casi non espressamente contemplati, ma comunque rilevanti rispetto alla corretta erogazione del servizio.

L'importo complessivo delle penali irrogate ai sensi dei commi precedenti non può superare il 10 % dell'importo contrattuale aggiudicato. Qualora le inadempienze siano tali da comportare il superamento di tale importo trova applicazione quanto previsto in materia di risoluzione del contratto.

Il provvedimento applicativo della penale sarà assunto dall'Amministrazione e comunicato all'Aggiudicatario. L'importo relativo all'applicazione della penale, esattamente quantificato nel provvedimento applicativo della stessa penalità, verrà detratto dal pagamento della fattura emessa.

9. Risoluzione per grave inadempienza – clausola risolutiva espressa

Nel caso di inadempienze gravi e/o ripetute agli obblighi previsti dal presente capitolato, diversi da quelli già previsti dall'articolo precedente, il Comune ha la facoltà, previa contestazione scritta, di risolvere il contratto, ai sensi degli articoli 1453 e 1454 del codice civile, con tutte le conseguenze di legge che la risoluzione comporta.

Ai fini del presente comma, si intendono inadempienze gravi:

- l'inosservanza degli obblighi derivanti dalla qualifica di RDP di cui al punto 7.1;
- il mancato e reiterato aggiornamento tempestivo dei registri di cui al punto 7.7;
- lo svolgimento dei doveri derivanti dal presente incarico senza la necessaria diligenza e perizia tecnica e giuridica, richiesta dalla peculiarità del servizio, che abbia comportato rilievi o sanzioni ad opera delle Autorità competenti al controllo;
- la cessazione o la sostituzione del RDP.

Si applicano alla risoluzione del contratto i principi del giusto procedimento previsti all'art.8.

10. Obbligo di tracciabilità dei flussi finanziari

L'aggiudicatario assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'art. 3 della L. 13.8.2010, n. 136 e ss.mm.ii. e si impegna a dare immediata comunicazione alla stazione appaltante e alla Prefettura-Ufficio Territoriale del Governo di Napoli della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.