AFFIDAMENTO DEI SERVIZI PER L'ATTUAZIONE DEL REGOLAMENTO U.E n. 679/2016 SULLA PROTEZIONE DEI DATI PERSONALI E INDIVIDUAZIONE DEL RESPONSABILE PROTEZIONE DATI (RPD)

DISCIPLINARE TECNICO

1. Indicazioni generali

Il Regolamento UE 679/2016 detto anche RGPD sulla protezione dei dati personali comporta per le pubbliche amministrazioni una riorganizzazione interna che presuppone la ricognizione, la valutazione e l'eventuale adeguamento delle misure di sicurezza normative, organizzative e tecnologiche, già adottate dagli enti a tutela della privacy, e che si articola nelle seguenti fasi:

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

L'adeguamento alle nuove norme, i correttivi e i miglioramenti necessari all'attuale livello di sicurezza del trattamento dei dati presuppongono il possesso di competenze informatiche e giuridiche con particolare riguardo al diritto amministrativo, alla legislazione degli enti locali ed alle norme sulla tutela dei dati personali: le competenze giuridiche sono documentabili dal possesso della laurea in materie giuridiche e dall'esperienza lavorativa maturata presso enti locali o altre pubbliche amministrazioni, in qualità di dipendenti, consulenti o collaboratori.

Le competenze informatiche, con particolare riguardo alla gestione di sistemi informativi complessi, afferenti alla gestione di servizi pubblici o privati comportanti il trattamento di dati sono documentabili dal possesso di titolo di studio adeguato e dall'esperienza lavorativa maturata presso aziende private, enti locali o altre pubbliche amministrazioni, in qualità di dipendenti, consulenti o collaboratori nel settore informatico.

2. Organizzazione amministrativa dell'ente

L'ente è organizzato nelle seguenti sette aree assegnate a responsabili titolari di P.O:

- Affari Generali
- Finanziaria
- Lavori Pubblici
- Sviluppo e tutela del territorio
- Servizi alla Persona
- Servizi culturali
- Polizia Municipale

Le aree Vigilanza, Servizi Culturali e Servizi alla Persona sono dislocate in tre sedi diverse.

3. Trattamento dei dati

Ciascuno degli uffici e dei servizi indicati svolge attività comportanti il trattamento di dati personali di cittadini, utenti, contribuenti, fornitori, dipendenti. In alcuni limitati casi vengono trattati anche dati sensibili.

Il trattamento viene effettuato per lo più con modalità informatizzate, con specifici programmi gestionali in rete. In molti casi è presente anche un archivio cartaceo.

I trattamenti più importanti e significativi prescindono 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 ed urbanistica.

Altri trattamenti, anche di dati sensibili, 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) oppure sono connessi alla necessità di utilizzare determinate procedure, previste per legge, che richiedono il trattamento di dati sensibili o giudiziari (es. gare di appalto) oltre ai trattamenti riguardanti la gestione del proprio personale dipendente.

4. Organizzazione informatica

L'ente è dotato di CED. La dotazione dei computer dell'ente consta, oltre che di 4 differenti reti di computer locali (LAN), di una rete geografica che si appoggia su linee ADSL (VPN) e permette il collegamento della sede principale (viale Vittoria, 14 Alpignano) con le due sedi decentrate (biblioteca in via Matteotti 2, Polizia Municipale in piazza Vittorio Veneto 1 e Servizi alla Persona in via Boneschi 11). Il Comune si avvale di:

- servizi web (e-mail con anti-virus ed anti-spam, spazio web, servizio di firewall e gestione di una DMZ)
- servizi wifi integrati con il servizio internet dell'Ente
- un ponte radio per il collegamento del CED con gli uffici dislocati in via Boneschi, 11.

Come sopra premesso gli uffici sono dislocati in quattro sedi fisicamente diverse, servite da una configurazione di firewall e di router sia per instradare i dati dalle sedi decentrate verso i server del CED sia per impedire l'accesso alla rete comunale dall'esterno.

Il sistema hardware dell'ente consta di n. 67 personal computer con sistemi operativi diversi (Windows XP/7/10) distribuiti nelle quattro sedi comunali. Nella sede centrale si trova la maggior parte dei computer collegati in rete su 4 server dedicati nella sede centrale di Viale Vittoria e n. 2 server nelle sedi decentrate. Nella biblioteca in via Matteotti 2 la condivisione è assicurata da una rete peer to peer.

Il riconoscimento delle login è assicurato nella sede centrale da un sistema di active directory (Windows 2000), mentre nelle sede decentrate il riconoscimento è gestito da computer locali, ovvero da un server con active directory su un Windows server 2003 r2 (Polizia municipale) e da un computer con Windows 7 Pro per la sede di via Boneschi 11.

La procedura di backup è assicurata dal riversamento quotidiano di tutti i file dell'Ente in due supporti magnetici rimovibili (hard disk esterno) e di un server NAS in rete in cui vengono riversati i suddetti dati con periodicità settimanale; esiste un ulteriore NAS a disposizione dell'area Polizia Municipale per il backup dei dati in rete (la procedura è notturna e quotidiana).

I software in licenza d'uso per la gestione della maggior parte delle attività comunali sono di Siscom SpA, Maggioli SpA e AP Kappa srl e risiedono su due database differenti : Ms Sql-Server (Siscom e AP Kappa) e Postgres (Maggioli). Sono presenti inoltre i software ministeriali previsti per legge.

Il firewall è di tipo NAT ed è gestito direttamente dalle politiche di accesso nell'hardware del router che forniscono la connettività internet e permettono la VPN tra le sedi.

Gli antivirus sono in parte forniti dal sistema operativo (per i computer con Windows 10 e 7) ed in parte dal software AVG antivirus installato su un server di produzione collocato presso i locali del C.E.D per i 16 computer Windows XP pro (in corso di sostituzione con computer Windows 10 pro).

Esistono due servizi esternalizzati: il sito internet attualmente in hosting presso EPUBLIC che prevede una raccolta di dati personali per il servizio di newsletter.

La Polizia Municipale può accedere alle registrazioni dei sistemi di videosorveglianza dislocati in varie aree del territorio comunale.

L'assistenza e la manutenzione informatica hardware sono prevalentemente interne, mentre quelle software sono prevalentemente esternalizzate.

5. Oggetto dell'incarico

Le attività che l'ente intende affidare all'esterno e sulla base delle quali dovrà essere formalizzata l'offerta, sono:

- funzione di RPD - assegnata a soggetto in possesso di laurea magistrale (vecchio ordinamento) o diploma di laurea specialistica (nuovo ordinamento) in giurisprudenza o equipollente - per il periodo di due anni decorrenti dalla nomina: per lo svolgimento della funzione è richiesta la presenza del RPD presso l'ente e pertanto non è ammessa la consulenza e/o la prestazione online;
- supporto e assistenza alla mappatura dei processi per individuare quelli collegati al trattamento dei dati personali
- individuazione tra i processi risultanti dalla mappatura di quelli che presentano rischi, con una prima valutazione degli stessi in termini di maggiore o minore gravità
- supporto e assistenza alla mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento
- 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;
- interventi formativi del personale di cui almeno in house
- predisposizione del registro dei trattamenti di dati personali e del registro delle categorie di attività
- proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni
- valutazione di impatto sulla protezione dei dati.

La prestazione del servizio avrà durata biennale (24 mesi) e un compenso annuo, al netto del ribasso offerto, non superiore a € 8.000,00 IVA esclusa.

6. Nomina del RPD

La nomina del RPD avrà decorrenza dalla data di conferimento dell'incarico e di nomina e avrà durata biennale.

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 effettuano il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre normative relative alla protezione dei dati. Ai fini del presente compito il RPD deve indicare ai Titolari 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 GDPR e delle altre normative relative alla protezione dei dati, fermo 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 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. 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 indispensabili al raggiungimento degli obiettivi previsti dal legislatore europeo.

L'indagine deve essere quindi svolta in maniera puntuale, settore per settore, sulla base di check list fornite dai professionisti incaricati; i responsabili dei singoli servizi forniranno tutte le informazioni richieste, acquisendole a loro volta dai fornitori esterni, qualora non siano a disposizione dell'ente.

Le attività suddette devono concludersi entro i termini che saranno stabiliti successivamente al conferimento dell'incarico.

8. 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 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 altresì misure tecniche ed organizzative i sistemi di autenticazione, i sistemi di autorizzazione, i sistemi di protezione (antivirus, firewall, antintrusione, altro), le misure antincendio, i sistemi di rilevazione di intrusione, i sistemi di sorveglianza, i sistemi di protezione con videosorveglianza, la registrazione degli accessi, la verifica dell'esistenza di porte, armadi e contenitori dotati di serrature e ignifughi, i sistemi di copiatura e conservazione di archivi elettronici e altre misure per ripristinare tempestivamente la disponibilità e l'accesso dei dati in caso di incidente fisico o tecnico.

L'elaborazione del piano di adeguamento deve essere presentata 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 ed integrazioni concordate, e consegnata la relazione definitiva.

9. Formazione del personale

Gli interventi formativi del personale, almeno uno all'anno da svolgersi *in house*, devono prevedere una formazione di base di tutti i dipendenti, e di 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 8, 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 Segretario comunale o il Responsabile di area competente.

10. Predisposizione 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 ed 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, 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 ed organizzative del trattamento adottate

h) il 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 ed 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 RPD non appena conclusa la fase di mappatura prevista al punto 7.

La tenuta e l'aggiornamento dei registri sarà a cura del RPD che dovrà provvedervi tempestivamente. Con cadenza semestrale i registri dovranno essere sottoposti al controllo ed alla vidimazione, rispettivamente:

- per quanto riguarda il registro dei trattamenti, al titolare del trattamento o suo delegato
- per quanto riguarda il registro delle categorie di attività trattate, ai responsabili dei servizi competenti.

11. Proposta di adeguamento della modulistica in uso agli uffici

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.

12. 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 del GRDP, considerati la natura, l'oggetto, il contesto e le finalità dello stesso trattamento.

Il Titolare si avvale della consulenza tecnica del RPD, il quale dovrà entro 15 giorni dalla richiesta 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 che permetta di realizzare e dimostrare la conformità alle norme del trattamento di cui trattasi.

13. Inadempimento e ritardo. Penalità

Il ritardo nell'esecuzione delle prestazioni indicate ai paragrafi 7, 8, 9 e 10 comporterà l'applicazione di una penale 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 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 articoli 1453 e 1454 del codice civile, con richiesta di risarcimento dei danni.

L'applicazione della penale sarà preceduta da formale contestazione scritta a cui il RPD potrà presentare le proprie controdeduzioni nel termine indicato nella contestazione, non inferiore a 10 giorni dalla data del ricevimento della contestazione stessa.

Qualora, entro il termine stabilito, non sia pervenuta alcuna motivata giustificazione scritta, ovvero qualora le stesse non siano ritenute fondate, il Comune applicherà le penali previste, motivando il mancato accoglimento delle giustificazioni.

Non è comunque precluso al Comune il diritto di sanzionare eventuali casi non espressamente contemplati comunque rilevanti rispetto alla corretta prestazione del servizio. Qualora le inadempienze siano tali da comportare il superamento dell'importo contrattuale si procederà alla 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.

14. Risoluzione per grave inadempienza. Clausola risolutiva espressa

Nel caso di inadempienze gravi e/o ripetute agli obblighi previsti dal presente disciplinare e diversi da quelli già previsti dal paragrafo precedente, il Comune ha 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. Si intendono inadempienze gravi:

- l'inosservanza degli obblighi derivanti dalla qualifica di RPD
- il mancato e reiterato aggiornamento tempestivo dei registri
- 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 RPD

Si applicano alla risoluzione del contratto i principi del giusto procedimento già previsti al paragrafo precedente in materia di irrogazione delle penali.

15. Obbligo di tracciabilità dei flussi finanziari

All'incarico si applicano tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136 e successive modifiche inclusa l'immediata comunicazione all'ente e alla Prefettura-Ufficio Territoriale del Governo di Torino della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.