COMUNE DI VITTUONE
Città Metropolitana di Milano
Piazza Italia, 5 – 20010 VITTUONE
P.IVA/C.F. 00994350155

CONFERIMENTO DELL'INCARICO PER L'ATTUAZIONE DEL REGOLAMENTO U.E n. 679/2016 SULLAPROTEZIONE DEI DATI PERSONALI ED 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.

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 inciderà 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 sia dal punto di vista 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 deve essere inteso non come mero "adempimento" ma come 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 ed i miglioramenti necessari. L'attività da svolgere presuppone quindi l'incrocio di competenze informatiche e giuridiche difficilmente riscontrabili in una sola professionalità. Si ritiene quindi necessario che il gruppo di lavoro da adibire all'incarico sia composto da soggetti in possesso delle seguenti competenze:

- comprovate competenze giuridiche, con particolare riguardo al diritto amministrativo, alla legislazione degli enti locali ed alle norme sulla tutela dei dati personali; le competenze 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.
- 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; le competenze 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 in 5 settori, a capo dei quali sono posti delle Funzioni dirigenziali:
Settore Affari Generali e Sociali
Settore Finanziario ed Educazione
Settore Lavori Pubblici, Sport e Tempo Libero
Settore Edilizia Privata, Urbanistica e Commercio
Settore Gestione Sicurezza del Territorio
L'ente non è dotato di un Centro Elaborazione Dati (Ced) e si avvale dei servizi specializzati esterni.

3. Ubicazione fisica degli uffici e servizi

Gli uffici ed i servizi dell'ente sono dislocati in diverse strutture:

- sede centrale in Piazza Italia, n. 5 – Settore Affari Generali e Sociali, Settore Finanziario ed Educazione, Settore Lavori Pubblici, Sport e Tempo Libero, Settore Edilizia Privata, Urbanistica e Commercio;
- sede di Via Petrarca, n. 5 - Settore Gestione Sicurezza del Territorio
- sede di Via Milano – Biblioteca (

4. Trattamenti di dati

Ciascuno degli uffici e servizi indicati svolge attività e compiti che comportano 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, ma in molti casi 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 ed urbanistica;
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, vi è tutto l'universo dei dati personali trattati nella gestione del proprio personale, che contengono al loro interno anche dati sensibili.

5. Organizzazione informatica

Il sistema informatico comunale consta di n. 43computer con s.o. windows 7 e windows 10.
Nella sede centrale si trovano la maggior parte dei computer, collegati in rete per mezzo di switch in armadio centralizzato su 2 piani differenti e 2 sedi differenti (Anagrafe Polizia locale e Biblioteca)
I pc degli utenti comunali sono collegati in rete con un dominio gestito dai server installati nella sala CED.

Sala CED

Nella sala ced, accessibile solo con chiave, sono ospitati i server comunali, alcuni fisici ed altri virtualizzati, quest'ultimi installati su un sistema clustering vmware.
I server virtualizzati sono 5:
1. server con i programmi della APKAPPA per la gestione degli applicativi. Risiede sullo stesso il database MySqlcontenente tutti i dati comunali (windows 2008).
2. server per la gestione della posta elettronica e dei dati.Risiede sullo stesso il database MSSqlcontenente tutti i dati comunali (windows 2008).

3. server per la gestione dell'active directory (windows 2008).
4. Server firewall ENDIAN 3.0 a protezione della rete interna.
5. Server dedicato alle pubblicazioni dell'albo on line

Abbiamo poi i sistemi di backup:
1. nas per la gestione del backup in sede distaccata
2. dischi USB su cui vengono eseguiti ulteriori procedure di backup.

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:

1. nomina del RDP per il periodo di due anni;
2. supporto e assistenza alla mappatura dei processi, per individuare quelli collegati al trattamento dei dati personali;
3. 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
4. supporto e assistenza alla mappatura degli incarichi dei soggetti coinvolti nel trattamento e dei livelli di responsabilità, ed eventuale aggiornamento;
5. 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;
6. interventi formativi del personale;
7. predisposizione del registro dei trattamenti di dati personali e del registro delle categorie di attività;
8. proposta di adeguamento della modulistica in uso agli uffici, qualora non conforme alle nuove disposizioni;
9. 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 biennale.

Compiti del Responsabile della Protezione dei Dati

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 la 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 ed 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. Ai fini del presente compito il RPD deve indicare al 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 RGPD 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;

7.2 -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 partenza per definire la situazione di partenza e la strada da percorrere per raggiungere gli obiettivi previsti dal legislatore europeo.
L'indagine deve essere quindi svolta in maniera accurata, settore per settore, sulla base di check list fornite dai professionisti incaricati; i responsabili dei singoli servizi forniranno il supporto necessario, fornendo tutte le informazioni richieste, acquisendole a loro volta dai fornitori esterni, qualora non siano a disposizione dell'ente.
Le attività previste devono concludersi entro 15 giorni naturali e consecutivi dal conferimento dell'incarico.

7.3. 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; 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.*
L' attività prevista 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.

7.4. Interventi formativi del personale

Gli interventi formativi del personale devono prevedere una formazione di base, da impartire a 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 7.3, 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 di Settore competente.

7.5. 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, 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 ed 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 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 RDP, non appena conclusa la fase di mappatura prevista al punto 7.2.

La tenuta e l'aggiornamento dei registri sarà a cura del RDP 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 dirigenti dei servizi competenti

7.6. 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 e**ntro due mesi dalla data di scadenza dei termini per la mappatura di cui al punto 7.2.**

7.7. 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 dovrà fornire i seguenti elementi, **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 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, e, 7.5 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 articoli 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 7.5;
- 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 giusti procedimenti già previsti nell'articolo precedente in materia di irrogazione delle penali.

10. Obbligo di tracciabilità dei flussi finanziari

L'aggiudicatario assume tutti gli obblighi di tracciabilità dei flussi finanziari di cui all'articolo 3 della legge 13 agosto 2010, n. 136 e successive modifiche e si impegna a dare immediata comunicazione alla stazione appaltante ed alla Prefettura-Ufficio Territoriale del Governo della provincia di Milano della notizia dell'inadempimento della propria controparte (subappaltatore/subcontraente) agli obblighi di tracciabilità finanziaria.