COMUNE DI MALO
PROVINCIA DI VICENZA

DETERMINAZIONE N. 394
Data di registrazione 28/05/2018

Oggetto: REGOLAMENTO UE 679/2016 (GDPR). AFFIDAMENTO DEI SERVIZI DI ADEGUAMENTO DELL'ENTE ALLE DISPOSIZIONI RELATIVE ALLA PROTEZIONE DEI DATI PERSONALI.

VICE SEGRETARIO
IL RESPONSABILE DEL SERVIZIO

Visto il D.L.gs n. 118 del 23.06.2011 e successive integrazioni e modificazioni riguardante le disposizioni in materia di armonizzazione dei sistemi contabili e degli schemi di bilancio delle regioni, degli enti locali e dei loro organismi, a norma degli articoli 1 e 2 della legge 5 maggio 2009, n. 42;
Richiamata la deliberazione n. 85 in data 27.12.2017, dichiarata immediatamente eseguibile, con la quale il Consiglio Comunale ha approvato il Bilancio di previsione 2018-2020 ed i relativi allegati;
Richiamata la deliberazione di Giunta comunale n. 1 del 09.01.2018, dichiarata immediatamente eseguibile, con cui è stato approvato il PEG (Piano esecutivo di gestione) per gli anni 2018-2020;
Visto il decreto sindacale n. 1 in data 08.01.2018 con il quale è stato conferito al sottoscritto l'incarico di posizione organizzativa per l'anno 2018;

Premesso che:

- il Parlamento Europeo in seduta plenaria, il 14 aprile 2016, ha approvato il Regolamento generale sulla protezione dei dati, Regolamento UE 2016/679, anche noto come GDPR (General Data Protection Regulation), "Protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati" che costituisce, con la Direttiva (UE) 2016/680 del 27 aprile 2016 dello stesso Parlamento europeo e del Consiglio, il c.d. "pacchetto protezione dati personali";
- Il nuovo Regolamento è stato pubblicato sulla Gazzetta Ufficiale Europea del 14 maggio 2016, è vigente dal 24 maggio 2016 ed applicabile a decorrere dal 25 maggio 2018 in tutti gli Stati membri; tale applicabilità ha il fine di trattare in modo omogeneo il tema della privacy sia nelle aziende private che presso le amministrazioni pubbliche dei diversi Paesi che compongono l'Unione;
- Il predetto Regolamento prevede che tutte le Pubbliche Amministrazioni (ad eccezione delle autorità giudiziarie) dovranno obbligatoriamente adeguarsi entro la data di applicazione e cioè entro il 25 maggio p.v.;

Dato atto che la nuova normativa europea attua un profondo mutamento culturale e, perciò, quanto richiesto agli Stati membri non può limitarsi alla osservanza di un mero adempimento formale in materia di privacy, ma deve porsi nella prospettiva di adeguare le norme di protezione dei dati ai cambiamenti determinati dalla continua evoluzione delle tecnologie;

Considerate le principali novità introdotte dal RGPD, che riguardano in particolare:

- il recepimento del “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 idonee per garantire un livello di sicurezza adeguato al rischio, stabilendo che i trattamenti siano conformi ai principi e alle disposizioni del Regolamento;
- L’introduzione della responsabilità diretta dei titolari del trattamento in merito al compito di assicurare ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali;
- La definizione della nuova categoria di dati personali (i c.d. dati sensibili di cui al precedente Codice Privacy);
- L’istituzione della figura obbligatoria del Responsabile della protezione dei dati -“Data Protection Officer”(DPO), incaricato di assicurare una gestione corretta dei dati personali negli enti;
- L’introduzione del Registro delle attività del trattamento in forma scritta o anche in formato elettronico, ove sono descritti i trattamenti effettuati e le procedure di sicurezza adottate e che dovrà contenere specifici dati indicati dal RGPD;
- L’obbligo, a carico dell’ente, di effettuare la valutazione di impatto sulla protezione dei dati, prima di procedere al trattamento, soprattutto quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche;
- La reintroduzione dell’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;
- Il rafforzamento dei poteri delle Autorità Garanti nazionali e l’inasprimento delle sanzioni amministrative a carico di imprese e pubbliche amministrazioni in caso di violazioni dei principi e disposizioni del Regolamento;

Ricordato che il primo obbligo a cui l’Amministrazione è tenuta riguarda l’individuazione della nuova figura del Responsabile della protezione dei dati personali che va “coinvolto in tutte le questioni riguardanti la protezione dei dati personali”;

Rilevato che il Responsabile deve essere individuato, se possibile, all’interno dell’Ente fra il personale dipendente in possesso di requisiti di competenza oltre che in posizione di terzietà, nel senso di non essere direttamente coinvolto in processi di trattamento dei dati, e che, solo in caso di assenza, può essere scelto mediante affidamento all’esterno, in base a un contratto di servizi;

Ritenuto di avvalersi di un professionista esterno, in quanto la dotazione organica è carente di figure professionali in possesso dei requisiti previsti per l'espletamento dell'incarico avente ad oggetto le seguenti prestazioni:
- Adeguamento al Regolamento Europeo (UE) 2016/679 dell’organizzazione aziendale;
- Adozione di tutti gli accorgimenti tecnici necessari a garantire la compilazione dei trattamenti, anche sotto il profilo della sicurezza in capo al titolare e responsabile del trattamento dei dati, secondo il Regolamento;
- Procedure atte a costituire uno strumento efficace per il titolare a fronte della responsabilità di rendicontazione o di "accountability";
- Nomina Data Protection Officer (DPO);
- Configurazione e mantenimento di un Sistema di Gestione Privacy secondo quanto previsto dal GDPR;

Vista l'indagine di mercato condotta da Pasubio Tecnolgia, i cui risultati sono stati trasmessi al Comune di Malo, con nota prot. 9781 del 3/5/2018;

Dato atto che il servizio offerto che meglio si adatta alle esigenze del Comune di Malo, risulta essere quello proposto dalla ditta Regola Team Srl, con sede a Porcia (PN) in Via Forniz n.15;

Vista la vigente normativa che disciplina la materia dei contratti pubblici ed in particolare:
- l’art. 37, comma 1, del D.Lgs. 50/2016, in materia di aggregazione e centralizzazione della committenza, che prevede la possibilità per le stazioni appaltanti di procedere autonomamente all'acquisizione di forniture e servizi di importo inferiore ad € 40.000,00;

- l'art. 36, comma 2, lettera a), del D.Lgs 50/2016, che prevede la possibilità di ricorrere all'affidamento diretto per servizi di importo inferiore ad € 40.000,00;

Considerato che il costo stimato dei servizi da acquisire è inferiore alle soglie di rilevanza comunitaria ex art.35 del D.Lgs.50/2016;

Ritenuto di acquisire i servizi in oggetto mediante affidamento diretto sul MEPA, ai sensi dell'art. 36 comma 2 lettera a) del D.Lgs 50/2016 in considerazione dell'importo stimato della fornitura inferiore ad € 40.000,00 euro, nel rispetto dei principi di economicità, efficacia, tempestività, proporzionalità, non discriminazione, rotazione, pubblicità e trasparenza;

Dato atto che è stata attivata la trattativa diretta di acquisto con la ditta *Regola Team Srl*, presente sul Mercato Elettronico della Pubblica Amministrazione, nell'ambito del Bando "Servizi/Servizi supporto specialistico", valutata l'esperienza e la professionalità di detta ditta in detto settore merceologico, ponendo a base della procedura l'importo stimato di € 10.000,00 (IVA esclusa), per anni 1 (uno), con possibilità di rinnovo per ulteriori anni 2 (due);

Visto l'offerta MEPA della ditta *Regola Team Srl,* n. 273753 in data 25/5/2018, che per i servizi richiesti ha offerto i prezzo a corpo di € 9.200,00 oltre IVA di legge:

Ritenuto congruo il prezzo offerto e pertanto di affidare a detto operatore economico i servizi in oggetto impegnando la relativa spesa;

Dato atto che l'efficacia di detto affidamento e la stipula del relativo contratto, come allegato sub A), rimane subordinata alla verifica positiva del possesso in capo all'aggiudicatario dei requisiti prescritti dalla legge e all'attestazione di assenza di motivi di incompatibilità od inconferibilità ai sensi dell'art. 15 del DLgs 33/2013 e dell'art 20 del DLgs 39/2013;

Preso atto che il contratto sarà sottoscritto in modalità elettronica, come previsto dall'art. 32, comma 14, del D.Lgs 50/2016, avrà durata annuale, a decorrere dalla data di sottoscrizione, con possibilità di rinnovo per altri 2 (due) anni;

Ritenuto di impegnare la spesa complessiva di € 11.224,00 (€ 9.200,00 + € 2024,00 di IVA 22%) nel bilancio di previsione 2018-2020, come segue:
- € 5.612,00 Cap. 5612 anno 2018;
- € 5.612,00 Cap. 5612 anno 2019;

Verificato, ai sensi dell'art. 9, comma 1, lett. a), numero 2 del D.L. 78/2009, convertito con L. 102/2009, il preventivo accertamento della compatibilità del programma dei pagamenti conseguente al presente atto con le regole di finanza pubblica e la programmazione dei flussi di cassa;

Visto il D.Lgs 50/2016;
Visto il D.Lgs. n. 267 del 18.08.2000;
Visto lo Statuto Comunale ed il Regolamento per l'ordinamento degli uffici e dei servizi;

D E T E R M I N A

1) di affidare alla ditta Regola Team Srl, con sede a Porcia (PN) in Via Forniz, 15 – C.F. 01321160937, i servizi di adeguamento dell'ente alle disposizioni relative alla protezione dei dati personali, come sotto indicati, per l'importo complessivo di € 11.224,00 (€ 9.200,00 + € 2024,00 di IVA 22%):

Attività tecniche IT e di supporto al Sistema di Gestione Privacy:
Attività di indagine, analisi e rilevazione degli aspetti sulla conformità delle aziende alle norme vigenti:
- Rilevazione dei dati dell'organizzazione, compreso il settore e il nome del rappresentante legale;
- Rilevazione/Indagine sullo stato di conformità dell'organizzazione alle norme privacy e di altre informazioni utili ai fini Privacy;
- Rilevazione dei trattamenti effettuati al momento della rilevazione;
- Rilevazione degli Asset intesi come beni materiali, immateriali, banche dati in possesso dell'organizzazione;

- Rilevazione dei membri coinvolti nel trattamento compresi dipendenti, collaboratori, fornitori che hanno, a qualsiasi titolo, accesso, diretto o indiretto, alle informazioni oggetto del trattamento;
- Rilevazione dei compiti svolti dai membri indicati al punto precedente;
- Censimento dei rischi e censimento delle misure adottate per la riduzione del rischio.

Implementazione Sistema Privacy con produzione di Istruzioni Procedure e Moduli:
- Registro dei Trattamenti con esempi e modelli di riferimento;
- Membri privacy(tutti i soggetti che partecipano come incaricati o responsabili al sistema privacy);
- Asset (Applicazioni, Database, Archivi che contengono dati personali);
- Enterprise Risk Assessment, sistema di Risk analysis per la rilevazione degli impatti, minacce e calcolo residuo di rischio informatico o fisico;
- PIA (Privacy Impact Assessment);
- Procedure (Diritti Interessati, Privacy by Design/ Default, Data Breach);
- Registro Data Breach;
- Audit pianificati con verifica dell'operato dell'Amministrazione di Sistema, verifica dell'operato del Database Administrator, verifica del mantenimento dei backup, verifica sui backup e sulle simulazione di restore (disaster recovery), verifica misure minime anti intrusione e anti deperimento, verifica adeguamento misure minime sudispositivi WI-FI;
- Evidenze per le attività di Audit compiute;
- Esame dello stato della conformità alle norme privacy distinte;
Determinazione delle azioni da adottare per la conformità comprese evoluzioni del sistema informatico e di sicurezza per ogniarea d'intervento.

Descrizione del sistema privacy dell'organizzazione, implementazione del Sistema Privacy attraverso la configurazione delle componenti quali registro trattamenti, identificazione asset, membri del sistema privacy, membri del sistema,registro data breach, Privacy Impact Assessment (DPIA) dei trattamenti che presentano un rischio elevato per le libertà e i diritti degli interessati:
- Informativa per il trattamento condotto dall'organizzazione rivolto ai clienti, dipendenti, terzi;
- Registro dei Trattamenti;
- Enterprise Risk Management per la valutazione dei rischi relativi ad ogni Asset (database o applicazione);
- Identificazione dei trattamenti potenzialmente soggetti a PIA (Privacy Impact Assessment);
- Web Documents: Informativa, legge suiCookie;
- Asset, compresi i privilegi di accesso dei componenti del sistema privacy;
- Misure minime ADS -gestione macchina utente;
- Gestione della sicurezza della Rete Locale;
- Dismissione fisica di una macchina;
- Dismissione logica di una macchina;
- Backup;
- Conservazione delle copie logiche e cartacee;
- Disaster Recovery e Business Continuity;
- Gestione delle credenziali di accesso: evidenze di consegna;
- Backup log dei sistemi interni e/o esterni all'organizzazione;
- Procedura gestione interruzioni pregresse (procedura di verifica periodica).

Attività legislative ed adeguamento documentale:
- Produzione di tutti i documenti prescritti dal GDPR: informative privacy, consulenza relativa alla stesura e tenuta del registro dei trattamenti, redazione dei contratti di nomina deiresponsabili e degli incaricati al trattamento, procedure relative all'esercizio dei diritti da parte degli interessati, procedure con controlli Privacy by Design/ by Default.
- Protocollo per il trattamento: revisione delle informative privacy ed adeguamento alle prescrizioni del GDPR, stesura dei contratti relativi alla nomina dei soggetti autorizzati comprensivi del protocollo per il trattamento dei dati, rivolta a dipendenti, fornitori (terze parti), collaboratori dell'organizzazione.
- Nomina ed incarico in veste di DPO della Dottoressa Anna Perut , con attività di sorveglianza e consulenza in accordo all'articolo 39 del Regolamento Europeo (UE) 2016/679;

Audit su procedure ed istruzioni pianificate:
- Privacy by Design/Default;
- Diritti degliInteressati;
- Data Breach;
- Nomina e revoca degli incaricati/responsabili;
- Adempimenti privacy relativi all'assunzione di un nuovo dipendente;
- Licenziamento o fine rapporto;
- La privacy nei rapporti di lavoro: codice di condotta del personale, privacy e uso di internet e della posta elettronica.

Eventuali richieste di assistenza e consulenza sui temi della privacy o formazione al personale;

2) di impegnare a tal fine la somma complessiva di €11.224,00, con la seguente imputazione nel bilancio di previsione 2018-2020:

ANNO DI IMPUTAZIONE	EURO	CAPITOLO/ ARTICOLO	CODICE CONTO FINANZIARIO(V LIVELLO)	ANNO DI ESIGIBILITÀ

2018	5612	236/04	U.1.03.02.11.999	2018
2019	5612	236/04	U.1.03.02.11.999	2019

3) CIG: Z2123C2460;

4) di attestare la congruità dei prezzi delle prestazioni oggetto del presente provvedimento;

5) di liquidare le somme dovute su presentazione di regolare fattura;

6) di dare atto che tutti i pagamenti a favore dell'affidatario saranno effettuati tramite bonifico bancario/postale su apposito conto corrente dedicato, indicato dallo stesso, come previsto dalla L. 136 del 13.08.2010, previa verifica della regolarità del servizio prestato e nei limiti dell'impegno di spesa assunto con il presente provvedimento.

*****

Si esprime parere favorevole di regolarità tecnica ai sensi dell'art. 147 bis del D.Lgs n. 267/2000.

Malo, 28/05/2018

IL RESPONSABILE DEL SERVIZIO
Oscar Raumer

(Documento firmato digitalmente)