



COMUNE DI FOIANO DELLA CHIANA
AREA "RAGIONERIA E TRIBUTI"

DETERMINAZIONE N° 474 DEL 21/05/2018

Cig Z6923AB57A

OGGETTO: SERVIZIO DI COMPILAZIONE DEL GDPR E NOMINA DPO. AFFIDAMENTO ED IMPEGNO DI SPESA

IL RESPONSABILE DELL'AREA INTESTATA

Tenuto presente che con decreto del Sindaco n. 1 del 02/01/2018, al sottoscritto sono state attribuite le funzioni di cui agli articoli 107 e 109 del decreto legislativo 18/8/2000, n° 267, relativamente all'area di posizione organizzativa denominata "Ragioneria e Tributi", a decorrere dal 01/01/2018 e sino al 30/06/2018;

Che - ai sensi del 2° comma dell'articolo 107 sopra richiamato - tali funzioni includono l'adozione degli atti e dei provvedimenti amministrativi, compresi tutti gli atti che impegnano l'Amministrazione verso l'esterno, nonché la gestione finanziaria, tecnica ed amministrativa, mediante autonomi poteri di spesa, di organizzazione delle risorse umane, strumentali e di controllo;

RITENUTA la propria competenza in merito all'assunzione del provvedimento, ai sensi:

- dell'articolo 107 suddetto;
- degli articoli 5 e 8 del "Regolamento sull'ordinamento degli Uffici e dei Servizi del Comune di Foiano della Chiana", approvato con deliberazione della Giunta n° 70 del 6.6.2000, esecutiva, e successive modifiche ed integrazioni;
- degli articoli 35 e 36 dello Statuto del Comune;

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 al proprio interno 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. Tutto questo prevedendo, 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;

Tutto ciò premesso;

Vista 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;

Visto il D.Lgs. n. 50/2016;

DATO ATTO, inoltre, che trattandosi di appalto di servizi pubblici di importo inferiore ad €. 40.000,00 (I.V.A. esclusa), per l'affidamento del relativo contratto possono trovare applicazione le disposizioni relative ai "Contratti sotto soglia UE" contenute nell'art. 36, comma 2, lett. a) del D.Lgs. n. 50/2016;

VISTO ANCORA l'art. 32 del D.Lgs. n. 50/2016 che al comma 14 dispone testualmente:

«Art. 32 (Fasi delle procedure di affidamento)

[...] 14. Il contratto è stipulato, a pena di nullità, con atto pubblico notarile informatico, ovvero, in modalità elettronica secondo le norme vigenti per ciascuna stazione appaltante, in forma pubblica amministrativa a cura dell'Ufficiale rogante della stazione appaltante o mediante scrittura privata in caso di procedura negoziata ovvero per gli affidamenti di importo non superiore a 40.000 euro mediante corrispondenza secondo l'uso del commercio consistente in un apposito scambio di lettere, anche tramite posta elettronica certificata o strumenti analoghi negli altri Stati membri.»;

DATO ATTO che in attuazione di quanto prescritto dal combinato disposto dell'art. 192 del D.Lgs. n. 267/2000 e dell'art. 32 del D.Lgs. n. 50/2016, nonché di quanto previsto dagli artt. 59 e 95 dello stesso D.Lgs. n. 50/2016, con la presente determinazione a contrattare devono essere definiti gli elementi essenziali del contratto da stipulare con l'operatore economico aggiudicatario;

CONSIDERATO che in relazione a quanto ammesso dall'art. 36, comma 2, lettera a), del D.Lgs. n. 50/2016 nel presente affidamento ricorrono i presupposti affinché il servizio, possa essere affidato direttamente ad un operatore economico in quanto sussistono le seguenti motivazioni tali da giustificare l'affidamento diretto del relativo contratto: rispetto della soglia massima di importo di €. 40.000 già sopra citata; economicità e tempestività della procedura di affidamento diretto;

Vista l'offerta rimessa dalla ditta allegata alla presente determinazione, per euro 3.000,00 oltre iva e ritenutala congrua e le cui attività sono riassunte come segue:

- 1 - CORSO DI FORMAZIONE "GDPR awareness" per tutti i dipendenti comunali;
- 2- IL SOFTWARE "GDPR FACILE" by Next in uso per la compilazione del GDPR;
- 3- ASSISTENZA TECNICA ALLA COMPILAZIONE del GDPR;
- 4- Nomina del responsabile di Next Duepuntozero S.r.l. dott. Marco Marcellini nel ruolo di Data Protection Officer (DPO);

Considerato che il servizio de quo, per la sua specialità, non è previsto su Mepa;

Ritenuto quindi, di procedere all'affidamento diretto del suddetto servizio alla ditta Next Duepuntozero S.r.l., che come da corrispondenza intercorsa con l'Ente ed allegata alla presente determinazione, si è dichiarata disponibile per l'importo di euro 3.000,00 + IVA 22%, per un totale di euro 3.660,00 iva compresa;

Appurata la regolarità del DURC;

D E T E R M I N A

Per le motivazioni meglio espresse in premessa, di impegnare la spesa totale di euro 3.660,00 IVA compresa al capitolo 1340 in favore di Next Duepuntozero S.r.l., a cui vengono affidati per l'anno 2018 i servizi meglio indicati in premessa e meglio evidenziati nell'allegata offerta;

Di rinviare a successivi atti di competenza della Giunta Comunale, la nomina del DPO;

Di rinviare a successivi atti, in seguito al ricevimento della fattura, la relativa liquidazione.

Foiano della Chiana, 21/05/2018
IL RESPONSABILE D'AREA
(F.to Luca Mazzi)
Firmato digitalmente