



FONDI
STRUTTURALI
EUROPEI
pon
2014-2020



Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia
scuolastica, per la gestione dei fondi strutturali per
l'istruzione e per l'innovazione digitale
Ufficio IV



ISTITUTO COMPRESIVO STATALE "VIA MAFFUCCI"

Cod. Mecc. MIIC8FP00T - C.F. 97667360156

e-mail: miic8fp00t@istruzione.it pec: miic8fp00t@pec.istruzione.it

Scuola Secondaria Primo Grado Via Maffucci, 60 - 20158 MILANO

☎02/88447160 – 02/88447164 fax

Scuola Primaria "M. Curie" Via Guicciardi, 1 - 20158 MILANO

☎02/88446931 – 02/39320412 fax

Scuola Primaria "G. Leopardi" V.le Bodio, 22 - 20158 MILANO

☎02/88446840 – 02/88446842 fax

Il Dirigente Scolastico

Visto il Regolamento di contabilità;

Visto il D.I. 44/2001;

VISTO il Decreto Interministeriale 1 febbraio 2001 n. 44, concernente le Istruzioni generali sulla gestione amministrativo-contabile delle istituzioni scolastiche

VISTO il Decreto Legislativo 30 marzo 2001, numero 165 recante Norme generali sull'ordinamento del lavoro alle dipendenze della Amministrazioni Pubbliche e ss.mm.ii.;

VISTA la legge 13 luglio 2015 numero 107, concernente la Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti;

VISTO l'articolo 36, comma 2, lett. a) del Decreto Legislativo 18 aprile 2016, numero 50, Attuazione delle direttive 2014/23/UE, 2014/24/UE e 2014/25/UE sull'aggiudicazione dei contratti di concessione, sugli appalti pubblici e sulle procedure d'appalto degli enti erogatori nei settori dell'acqua, dell'energia, dei trasporti e dei servizi postali, nonché per il riordino della disciplina vigente in materia di contratti pubblici relativi a lavori, servizi e forniture, nonché l'articolo 95, commi 4 e 5;

VISTO il Decreto Legislativo 19 aprile 2017, numero 56, recante Disposizioni integrative e correttive del Decreto Legislativo 18 aprile 2016, numero 50;

Richiamato il Codice dell'Amministrazione Digitale, D.Lgs. n. 82/2005, così come modificato dal D.Lgs. n. 179/2016, che all'art. 51, rubricato "Sicurezza dei dati, dei sistemi e delle infrastrutture delle pubbliche amministrazioni", prevede che "I documenti informatici delle pubbliche amministrazioni devono essere custoditi e controllati con modalità tali da ridurre al minimo i rischi di distruzione, perdita, accesso non autorizzato o non consentito o non conforme alle finalità della raccolta";

Preso atto che con Circolare del 18 aprile 2017, n. 2/2017, pubblicata in G.U. Serie Generale n. 103 del 5.05.2017, l'Agenzia per l'Italia Digitale (AGID), al fine di contrastare le minacce più comuni e frequenti cui sono soggetti i sistemi informativi delle Pubbliche Amministrazioni, ha disposto la sostituzione della circolare n. 1/2017 del 17 marzo 2017, recante "Misure minime di sicurezza ICT per le pubbliche amministrazioni" con nuove misure minime per la sicurezza informatica a cui le stesse Pubbliche Amministrazioni sono tenute a conformarsi entro il termine del 31.12.2017;

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:

- 1) 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;
- 2) 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;
- 3) 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;
- 4) 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;
- 5) disciplinata 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”;
- 6) 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;

Preso atto che l'art. 32, comma 2, del D.Lgs. n. 50/2016 (codice dei contratti) prevede la possibilità per le stazioni appaltanti di procedere all'affidamento di lavori, servizi e forniture di importo inferiore a 40.000 euro mediante affidamento diretto anche senza previa consultazione di due o più operatori economici;

Dato atto che il servizio in oggetto presenta rilevanti aspetti di carattere informatico e che, pertanto, nella fattispecie non trova applicazione l'art. 1, comma 502, della legge n. 208/2015, bensì l'art. 1, comma 512 della medesima normativa che testualmente prevede: *“Al fine di garantire l'ottimizzazione e la razionalizzazione degli acquisti di beni e servizi informatici e di connettività le amministrazioni pubbliche provvedono ai propri approvvigionamenti esclusivamente tramite gli strumenti di acquisto e di negoziazione di Consip Spa o dei soggetti aggregatori, ivi comprese le centrali di committenza regionali”*;

Dato atto che con la presente determinazione si intende affidare l'incarico per lo svolgimento del servizio volto all'adozione di provvedimenti e misure in ottemperanza alle disposizioni previste dal Regolamento (UE) 2016/679 in materia di protezione dei dati persona.

VERIFICATA la spesa necessaria e confrontati n°3 preventivi ricevuti;

CONSIDERATA congrua e più vantaggiosa l'offerta della ditta DIEMME INFORMATICA srl con sede legale a Marlia (LU) P.IVA 02115770469;

Ritenuto, per le motivazioni sopra esposte, di ricorrere alla procedura di affidamento diretto;

Considerato che la spesa pari a € 700,00 Iva esclusa può essere impegnata al capitolo P11 (Sicurezza) del piano esecutivo di gestione per l'anno 2018, gestione competenza;

Richiesto all'Autorità per la Vigilanza sui Contratti Pubblici (AVCP) opportuno codice identificativo di gara (CIG): [Z7A23BE615](#).

Per quanto sopra;

DETERMINA

1. Di aggiudicare per le motivazioni di cui in premessa, definitivamente e direttamente, alla ditta DIEMME INFORMATICA srl con sede legale a Marlia (LU) P.IVA 02115770469 l'esecuzione della fornitura in oggetto alle condizioni contenute nell'Ordine sopra citato;
2. Di affidare alla ditta DIEMME INFORMATICA srl con sede legale a Marlia (LU) P.IVA 02115770469, la fornitura dei servizi sopra citati;
3. Di impegnare la conseguente spesa pari a € 700,00 Iva esclusa al capitolo P11 (Sicurezza)
4. Di comunicare ai terzi interessati, da parte di questo ufficio, l'assumendo impegno di spesa sull'intervento suddetto;
5. Di individuare quale responsabile del procedimento per la corretta esecuzione di quanto determinato la Dott.ssa Laura Barbirato.
6. Di provvedere con separato atto alla liquidazione della fattura previa acquisizione del DURC secondo quanto previsto dall'art. 6 del D.P.R. 207/2010 e che tale certificato sarà obbligatoriamente allegato alla fattura nel rispetto delle disposizioni vigenti.

7. Di dare atto che il responsabile del procedimento ha proceduto nelle verifiche di cui all'art. 1 del D.L. n. 95/2012 convertito nella L. 135/2012 (spending review II), con l'esito indicato in premessa;

Milano, 25/05/2018
Prot. 0001973 VI.10

Il Dirigente Scolastico
Dott.ssa Laura Barbirato

A handwritten signature in black ink, reading "Laura Barbirato". The signature is written in a cursive style with some capital letters.