

Oggetto: Affidamento Servizio di Assistenza tecnico-Giuridica per l'attuazione del nuovo Regolamento europeo 2016/679 in materia di Privacy - GDPR

RELAZIONE ISTRUTTORIA

VISTA la legge 7 agosto 1990, n. 241 “Nuove norme in materia di procedimento amministrativo e di diritto di accesso ai documenti amministrativi” e ss.mm.ii.;

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:

- 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 informato 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 online) 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;

Preso atto che è stata effettuata indagine di mercato richiedendo preventivi per la predisposizione di tutta la documentazione nonché l'assegnazione della figura del DPO presso l'Azienda Speciale ASM Pomigliano;

Prendere atto che dall'indagine di mercato sono pervenuti n° 2 preventivi:

1. Associazione professionale Avv. Riccardo Imperiali e Avv. Rosario Imperiali, quale studio di consulenza legale, con prot. n° 634 del 22.06.2018 nella quale veniva indicata la disponibilità di impostare il sistema documentale, nonché il modello organizzativo, la formazione al personale e la suddivisione dei compiti al costo di €15.000,00 oltre IVA e C.N.A.P.
2. Società Maggioli SpA con prot. 723 del 16.07.2018 nella quale veniva indicata la disponibilità di impostare il sistema documentale, nonché il modello organizzativo, la formazione al personale e la suddivisione dei compiti al costo di €4.400,00 oltre IVA, nonché avere la designazione di GDO al costo di €1.600,00

Considerato che ai sensi dell'art.36, comma2, lettera a) del D.Lgs. n.50/2016, del Codice dei contratti, così come modificato dall'art.25, comma1, lett.b), n.1) del decreto correttivo D.Lgs. 19 aprile 2017, n.56, prevede la possibilità di stipulare contratti anche senza previa consultazione di due o più operatori economici;

Assegnare il CIG **Z4324DD871**

Tanto si trasmette per quanto di propria competenza


RUP
Dott. ing. Vincenzo Piscitelli

Il Dirigente

Visto il regolamento di ASM;

Visto il DLgs 50/2016 e le linee guida ANAC;

Letta e fatta propria la relazione istruttoria che è parte integrante della presente

Determina

1. Approvare la procedura negoziata intrapresa come da relazione istruttoria;
2. Affidare alla Società Maggioli SpA, con esede in via Emilia n°1555 – Sant'Arcangelo di Romagna (RN) PIVA 02066400405 il servizio di **Assistenza tecnico-Giuridica per l'attuazione del nuovo Regolamento europeo 2016/679 in materia di Privacy - GDPR;**

Pomigliano, 24.07.2018

Il Dirigente
Dott.ssa Maria Desolina Suppa

