



Ministero dell'Istruzione, dell'Università e della Ricerca  
**Istituto Istruzione Superiore "N. Miraglia"**

Istituti Associati  
Liceo Classico "N. Carlomagno" - Lauria  
Istituto Tecnico settore Tecnologico "E. Ferrari" - Lauria  
Liceo Scientifico Via Pietro Nenni - Rotonda

**Via Cerse dello speciale - 85044 LAURIA (PZ)**

Tel. 0973823966 Dirigente Scolastico 3939814291

Cod. MIUR: PZIS00600A – Cod. Fiscale 92000130762 - Codice Univoco Fatturazione Elettronica UF7YWT  
Sito internet: [www.iismiraglialauria.edu.it](http://www.iismiraglialauria.edu.it) e-mail: [pzis00600a@istruzione.it](mailto:pzis00600a@istruzione.it) – Pec: [pzis00600a@pec.istruzione.it](mailto:pzis00600a@pec.istruzione.it)

ISTITUTO D'ISTRUZIONE SUPERIORE - "N. MIRAGLIA"-LAURIA  
Prot. 0004369 del 13/07/2019  
06 (Uscita)

All'Albo dell'istituto  
Amministrazione trasparente

**Oggetto: Avviso interno/esterno per l'affidamento dell'incarico di "Responsabile della protezione dei dati personali" (Data Protection Officer- DPO) per gli adempimenti previsti dal Regolamento U.E 2016/679.**

### IL DIRIGENTE SCOLASTICO

- VISTA** la legge 15 marzo 1997 n. 59, concernente "Delega al Governo per il conferimento di funzioni e compiti alle Regioni ed Enti locali, per la riforma della Pubblica Amministrazione e per la semplificazione amministrativa";
- VISTO** il D.P.R. n. 275/1999, concernente norme in materia di autonomia delle istituzioni scolastiche;
- VISTO** il D.Lgs. n. 165/2001 recante "Norme generali sull'ordinamento del lavoro alle dipendenze delle Amministrazioni Pubbliche";
- VISTO** il D.I. n. 129 del 28/08/2018 "Regolamento concernente le istruzioni generali sulla gestione amministrativo-contabile delle istituzioni scolastiche";
- VISTO** il D. leg.vo n° 50 del 18/05/2016 "Codice dei contratti pubblici" e successive integrazioni e modifiche;
- VISTA** il regolamento d'istituto concernente le attività negoziali del Dirigente di cui alla Delibera del CdI n. 4 del 18/12/2018;
- VISTO** il Regolamento (UE) 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 «relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)», che introduce la figura del Responsabile dei dati personali (RDP) e in particolare la sezione 4:
- Articolo 37 - Designazione del responsabile della protezione dei dati
  - Articolo 38 - Posizione del responsabile della protezione dei dati
  - Articolo 39 - Compiti del responsabile della protezione dei dati;
- VISTE** le Linee-guida sui responsabili della protezione dei dati (RPD) -WP243 adottate dal Gruppo di lavoro, Art. 29, il 13 dicembre 2016 - Versione emendata e adottata in data 5 aprile 2017;
- VISTO** che il predetto Regolamento prevede l'obbligo per il titolare o il responsabile del trattamento di designare il Responsabile della protezione Dati «quando il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali» (art. 37, paragrafo 1, lett a);

**RECEPITO** che le predette disposizioni prevedono che il Responsabile della protezione Dati «può essere

un dipendente del titolare del trattamento o del responsabile del trattamento, oppure assolvere i suoi compiti in base a un contratto di servizi» (art. 37, paragrafo 6) e deve essere individuato «in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39» (art. 37, paragrafo 5) e «il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali trattati dal titolare del trattamento o dal responsabile del trattamento» (considerando n. 97 del *Regolamento generale sulla protezione dei dati*);

**CONSIDERATO**, al fine dell'attuazione del *Regolamento generale sulla protezione dei dati* (RGPD), le priorità operative indicate dal Garante privacy:

1. designazione del Responsabile della protezione dei dati (RPD, italianizzazione dell'acronimo DPO, Data Protection Officer, art. 37-39);
2. istituzione del Registro delle attività di trattamento (art.30 e cons. 171);
3. notifica delle violazioni dei dati personali ("data breach", art. 33 e 34) nonché la necessità mettere in atto gli ulteriori elementi attuativi introdotti dal RGPD;

**VISTO** che l'Istituzione scolastica è tenuta alla designazione obbligatoria del RPD nei termini previsti, rientrando nella fattispecie prevista dall'art. 37, par. 1, lett a) del RGPD ed è tenuta ad adempiere a quanto prescritto dal RGPD;

**CONSIDERATO** che si ritiene necessario esperire preliminarmente una indagine interna per verificare la disponibilità di personale idoneo ad assumere il suddetto incarico;

#### **EMANA**

il presente Avviso di selezione, che ha per oggetto l'assegnazione dell'incarico di Responsabile della protezione Dati (Data Protection Officer – DPO) e l'attività di assistenza e formazione su tutti gli adempimenti necessari per l'adeguamento alle disposizioni in quanto previsto dal RGPD.

#### **Art. 1 - Descrizione e caratteristiche della prestazione**

Le caratteristiche della prestazione oggetto dell'Avviso devono corrispondere alla descrizione di seguito esposta e il RPD dovrà ottemperare a quanto previsto nel Regolamento UE in epigrafe e in dettaglio. In particolare, dovrà:

1. informare e consigliare il titolare e il responsabile del trattamento, nonché i dipendenti, in merito agli obblighi derivanti dal Regolamento europeo e da altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati;
2. verificare l'attuazione e l'applicazione del Regolamento, delle altre disposizioni dell'Unione o degli Stati membri relative alla protezione dei dati nonché delle politiche del titolare o del responsabile del trattamento in materia di protezione dei dati personali, inclusi l'attribuzione delle responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento, e gli audit relativi;
3. fornire, se richiesto, pareri in merito alla valutazione d'impatto sulla protezione dei dati e sorvegliare i relativi adempimenti;
4. essere punto di contatto per gli interessati in merito a qualunque problematica connessa al trattamento dei loro dati o all'esercizio dei loro diritti;
5. fare da riferimento al Garante per la protezione dei dati personali oppure, eventualmente, consultare il Garante di propria iniziativa.
6. predisporre e monitorare l'aggiornamento del Registro delle attività di trattamento (art.30 e cons. 171), avviando quanto prima la ricognizione dei trattamenti svolti e delle loro principali caratteristiche (finalità del trattamento, descrizione delle categorie di dati e interessati, categorie di destinatari cui è prevista la comunicazione, misure di sicurezza, tempi di conservazione, e ogni altra informazione che il titolare ritenga opportuna al fine di documentare le attività di trattamento svolte) funzionale all'istituzione del registro. La ricognizione sarà l'occasione per verificare anche il rispetto dei principi fondamentali (art. 5), la liceità del trattamento (verifica dell'idoneità della base giuridica, artt. 6, 9 e 10) nonché l'opportunità dell'introduzione di misure a protezione dei dati fin dalla progettazione e per

- impostazione (privacy by design e by default, art. 25), in modo da assicurare, entro il 25 maggio 2018, la piena conformità dei trattamenti in corso (cons. 171);
7. collaborare con il titolare e il responsabile del trattamento dei dati alla notifica delle violazioni dei dati personali (“data breach”, art. 33 e 34);
  8. formare tutto il personale incaricato dell’area amministrativa in relazione al profilo di appartenenza di ciascun soggetto
  9. dar corso – in collaborazione con il titolare e il responsabile del trattamento dei dati - alla piena attuazione del RGPD, anche predisponendo un piano dettagliato di azioni.

## **Art. 2 - Caratteristiche del RPD**

Il RPD dovrà:

1. possedere: un’approfondita conoscenza della normativa e delle prassi in materia di privacy, nonché delle norme e delle procedure amministrative che caratterizzano lo specifico settore di riferimento; qualità professionali adeguate alla complessità del compito da svolgere, documentando le esperienze fatte, la partecipazione a master e corsi di studio/professionali.
2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.

## **Art. 3 - Durata dell’incarico**

L’incarico avrà la durata di dodici mesi (12 mesi) a decorrere dal 07/09/2019

Il presente contratto si intenderà comunque risolto in caso di abrogazione dell’obbligo per le scuole alla nomina del RPD. In tale evenienza si intenderà maturato e verrà corrisposto il compenso proporzionalmente al solo periodo di effettivo servizio.

## **Art. 4 - Istanza – Procedura di selezione**

Gli interessati dovranno far pervenire al Dirigente Scolastico istanza di partecipazione alla selezione, in busta chiusa (e controfirmata sui lembi di chiusura) riportante la dicitura: “*Avviso di selezione per il reclutamento di Responsabile per la protezione dei dati*”, entro le ore 9:00 del giorno 31/07/2019, consegnandola a mano ovvero tramite servizio postale presso l’Ufficio Protocollo di questa Istituzione Scolastica , ovvero facendola recapitare tramite pec [pzis00600a@pec.istruzione.it](mailto:pzis00600a@pec.istruzione.it). Le istanze di partecipazione, debitamente sottoscritte e corredate della Tabella valutativa, dovranno essere redatte in carta libera e corredate dalla seguente documentazione:

- Curriculum Vitae predisposto secondo il formato europeo, debitamente sottoscritto;
- Fotocopia del documento di riconoscimento del dichiarante, in corso di validità;
- Dichiarazione di assenza di incompatibilità per la copertura dell’incarico.

Nella domanda di partecipazione i candidati devono dichiarare sotto la loro responsabilità:

1. nome, cognome, luogo e data di nascita, cittadinanza, codice fiscale e/o partita IVA, comune di residenza, indirizzo e recapito telefonico;
2. di essere in possesso di certificata competenza e/o esperienza professionale maturata nel settore richiesto, prima della pubblicazione del presente bando;
3. di non avere condanne penali né procedimenti penali in corso, non essere stati destituiti da pubbliche amministrazioni e di essere in regola con gli obblighi di legge in materia fiscale; 4. di autorizzare il trattamento dei dati personali ai sensi della normativa vigente.

**Il Dirigente Scolastico si riserva di chiedere l’integrazione del curriculum vitae**, relativamente alle certificazioni originali delle esperienze e/o dei titoli dichiarati, e di effettuare verifiche a campione sulla reale sussistenza dei requisiti dichiarati dagli stessi candidati. La non veridicità di quanto sottoscritto comporterà l’automatica ed immediata esclusione dalla procedura di reclutamento. Il Dirigente Scolastico si riserva altresì di condurre controlli a campione al fine di verificare la veridicità dei contenuti delle dichiarazioni sostitutive, oggetto di valutazione.

Il Dirigente Scolastico si riserva di non attribuire l’incarico qualora vengano ritenuti non sufficienti i requisiti formali o professionali.

## Art. 5 - Criteri di valutazione e Assegnazione dell'incarico

L'assegnazione dell'incarico avverrà in base all'esito della redazione di elenchi graduati sulla base dei seguenti criteri:

### **Titoli di accesso: Laurea coerente con l'incarico**

<b>Titoli di studio</b>	<b>Punteggi</b>
Laurea in Informatica/Giurisprudenza	punti 20 per la votazione fino a 100/110 punti 15 per ogni voto da 101 a 110 punti 0,2 per la lode o tesi attinente all'incarico punti 3
Master / Specializzazioni, ulteriori lauree coerenti con l'incarico (ad es. Diritto dell'Informatica, Informatica giuridica)	punti 5 per ciascun titolo fino a un max di 15 punti
Precedenti documentate esperienze presso istituzioni scolastiche in qualità di data officer / Referente privacy	Punti 5 per ogni esperienza annuale fino ad un max di 25 punti
Precedenti esperienze presso istituzioni scolastiche in qualità di amministratore di sistema e nell'ambito della sicurezza informatica	Punti 5 per ogni esperienza annuale fino ad un max di 15 punti
Esperienze presso enti pubblici, aziende con riferimento al trattamento dati e/o alla sicurezza informatica	punti 5 per ogni esperienza annuale fino ad un max di 10 punti
Certificazioni possedute e (2 punti per ogni certificazione Eipass, Didasko; 4 punti per ECDL Avanzata; 4 punti ognuna se in possesso delle certificazioni Eipass Pubblica Amministrazione, Cybercrimes e IT security; 4 punti se in possesso della certificazione Microsoft DB Administrator)	Max 10 punti
Pubblicazioni, interventi a corsi, convegni come formatore/relatore, attinenti il tema della Privacy	1 punti per prestazione, max di 5 punti

## Art. 6 - Pubblicazione della Graduatoria

L'esame delle domande sarà effettuato dal Dirigente Scolastico sulla base della valutazione dei titoli di cui alla precedente tabella.

Saranno attribuiti i punteggi a ciascun candidato secondo quanto indicato nell'art. 5; saranno elaborate distintamente le graduatorie costituite per il personale interno – che avranno precedenza – ed esterno in assenza di personale interno - a parità di punteggio gli aspiranti candidati saranno graduati in base alla minore età.

L'esito della selezione sarà pubblicato all'albo on line di questa Istituzione scolastica e sul sito web [www.iismiraglialauria.edu.it](http://www.iismiraglialauria.edu.it)

Avverso la graduatoria è ammesso reclamo scritto, entro 5 giorni dalla data della sua pubblicazione. Trascorsi i 5 giorni senza reclami scritti, la graduatoria diventerà definitiva.

L'amministrazione si riserva di procedere al conferimento dell'incarico anche in presenza di una sola domanda pervenuta purché pienamente rispondente alle esigenze descritte nell'avviso Il Responsabile del procedimento è il Dirigente Scolastico.

## Art. 7 - Personale interessato

Il presente bando è indirizzato al personale docente ed ATA in servizio nell'Istituto e nell'amministrazione nonché a tutti i professionisti esterni.

## Art. 8 - Corrispettivo offerto

Il candidato, individuato ai sensi del presente avviso di selezione, sarà invitato a presentarsi presso l'Ufficio preposto, per l'attribuzione dell'incarico.

Compenso previsto: € 600,00 annuo, onnicomprensivi degli oneri di legge da corrispondersi in un'unica soluzione, al termine dell'attività, entro 30 gg. dalla presentazione di specifica relazione finale sulle prestazioni svolte, seconde le normative fiscali del caso..

**Art. 9 - Tutela della Privacy**

Il Responsabile del trattamento dati è il D.S.G.A.. I dati dei candidati saranno trattati nel rispetto del d.lgs. 196/03 e pertanto le stesse istanze degli aspiranti all'incarico dovranno contenere apposita dichiarazione di assenso al loro trattamento.

**Art. 10 - Pubblicità legale**

Il presente avviso è pubblicato all'Albo on line di questa Istituzione scolastica.

**IL DIRIGENTE SCOLASTICO**  
**Prof. Natale STRAFACE**

Firmato Digitalmente ai sensi del CAD e norme ad esso connesse



Allegato A - Tabella di valutazione dei titoli

Al Dirigente Scolastico  
Istituto d' Istruzione Superiore "Miraglia"  
LAURIA

Candidato: \_\_\_\_\_

***Titolo di accesso: Laurea coerente con l'incarico***

<i><b>Titoli di studio</b></i>	<i><b>Punteggi</b></i>	<i><b>Punteggio a cura dei dichiarante</b></i>
Laurea in Informatica/Giurisprudenza	Max punti 20	
Master, Specializzazioni, ulteriori lauree coerenti con l'incarico (ad es. Diritto dell'Informatica, Informatica giuridica)	punti 5 per ciascun titolo fino a un max di 15 punti	
Precedenti documentate esperienze presso istituzioni scolastiche in qualità di data officer / Referente privacy	Punti 5 per ogni esperienza annuale fino ad un max di 25 punti	
Precedenti esperienze presso istituzioni scolastiche in qualità di amministratore di sistema e nell'ambito della sicurezza informatica	Punti 5 per ogni esperienza annuale fino ad un max di 15 punti	
Esperienze presso enti pubblici, aziende con riferimento al trattamento dati e/o alla sicurezza informatica	punti 5 per ogni esperienza annuale fino ad un max di 10 punti	
Certificazioni possedute (2 punti per ogni certificazione Eipass, Didasko; 4 punti per ECDL Avanzata; 4 punti ognuna se in possesso delle certificazioni Eipass Pubblica Amministrazione, Cybercrimes e IT security; 4 punti se in possesso della certificazione Microsoft DB Administrator)	Max 10 punti	
Pubblicazioni, interventi a corsi, convegni come formatore/relatore, attinenti il tema	1 punti per prestazione, max di 5 punti	

FIRMA

\_\_\_\_\_