MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITÀ E DELLA RICERCA
Istituto Scolastico Comprensivo
"Giovanni XXIII"
Scuola dell'Infanzia e del 1° ciclo di istruzione
71037 – Monte Sant'Angelo (Fg) – Via Sant'Antonio Abate, 92
Cofisco: 83003020712 – **Cod. Mecc.**: FGIC83100Q – **Codice Univoco**: UFJLON
Tel.: 0884561316 **– Fax:** 0884568344 – **Sito web:** www.istitutogiovanni23.edu.it – **E-mail:** fgic83100q@istruzione.it-fgic83100q@pec.istruzione.it

Circ. n. 50

Monte Sant'Angelo, 19 gennaio 2019

Al Personale Docente e Ata
Sede

Agli Albi e agli Atti
Sul Sito web dell'Istituto

OGGETTO: **Incarico Responsabile della Protezione dei Dati Personali (RDP o DPO) ai sensi dell'art. 37 del regolamento UE 2016/679. Avviso interno.**

Con la presente si è a chiedere alle SS.LL. l'eventuale disponibilità a ricoprire l'incarico di **Responsabile della Protezione dei Dati Personali (RDP o DPO)** presso questa Istituzione, come di seguito indicato.

Art. 1 – Profilo del RDP o DPO

Il profilo del Data Protection Officer (DPO), figura di supporto al titolare o responsabile del trattamento nell'applicazione e per l'osservanza del Regolamento (UE) 679/2016, in conformità all'art. 37 (Designazione del Responsabile della protezione dei dati), è afferente a:

- Consulenti direzione
- Consulenti ed esperti di sistemi di gestione della sicurezza delle informazioni (norme ISO 27000)
- Auditor di sistemi di gestione
- Esperti di Risk Management
- Consulenti/esperti sulle normative attinenti alla privacy ed alla protezione dei dati personali (leggi, normative, disposizioni del Garante, ecc.)

Art. 2 – Requisiti richiesti

Si richiede il possesso dei seguenti requisiti, da documentare o autocertificare nel curriculum vitae ai sensi del DPR 445/2000:

a) Conoscenze:

- I principi di privacy e protezione dei dati by design e by default; i diritti degli interessati previsti da leggi e regolamenti vigenti; le responsabilità connesse al trattamento dei dati personali.
- Norme di legge italiane ed europee in materia di trattamento e di protezione dei dati personali
- Norme di legge in materia di trasferimento di dati personali all'estero e circolazione dei dati personali extra UE
- Le metodologie di valutazione d'impatto sulla protezione dei dati e PIA
- Le norme tecniche ISO/IEC per la gestione dei dati personali
- Le tecniche crittografiche
- Le tecniche di anonimizzazione
- Le tecniche di pseudonimizzazione
- Sistemi e tecniche di monitoraggio e "reporting"
- Gli strumenti di controllo per la produzione di documentazione
- I rischi critici per la gestione della sicurezza
- I tipici KPI (key performance indicators)
- La computer forensics (analisi criminologica di sistemi informativi)
- La politica di gestione della sicurezza e delle sue implicazioni con gli impegni verso gli utenti e i fornitori
- Le best practices e gli standard nella analisi del rischio
- Le best practices e gli standard nella gestione della sicurezza delle informazioni

- Le norme legali applicabili ai contratti
- Le nuove tecnologie emergenti
- Le possibili minacce alla sicurezza
- Le problematiche legate alla dimensione dei data sets (per esempio big data)
- Le problematiche relative ai dati non strutturati (per esempio data analytics)
- Le tecniche di attacco informatico e le contromisure per evitarli

b) Abilità:
- Contribuire alla strategia per il trattamento e la protezione dei dati personali
- Capacità di analisi
- Capacità organizzative
- Pianificazione e programmazione
- Analisi degli asset critici dell'Istituzione ed identificazione di debolezze e vulnerabilità riguardo ad intrusioni o attacchi
- Saper anticipare i cambiamenti richiesti alla strategia istituzionale dell'information security e formulare nuovi piani
- Saper applicare all'information security gli standard, le best practices e i più rilevanti requisiti legali
- Garantire che la proprietà intellettuale e le norme della privacy siano rispettate
- Negoziare termini e condizioni del contratto
- Preparare i template per pubblicazioni condivise
- Progettare e documentare i processi dell'analisi e della gestione del rischio
- Essere in grado di seguire e controllare l'uso effettivo degli standard documentativi dell'Istituzione

c) Competenze:
- Pianificazione di servizio
- Sviluppo di strategie per la sicurezza informatica
- Gestione dei contratti
- Sviluppo del personale
- Gestione del rischio
- Gestione delle relazioni
- Gestione della Sicurezza dell'informazione
- Governante dei sistemi informativi

d) Consolidata esperienza in ambito della sicurezza informatica (tecniche di attacco, crittografia, ecc.) e sui sistemi informatici e relativi database.

Art. 3 – Oggetto del servizio

Il Data Protection Officer (DPO), figura di supporto al titolare o responsabile del trattamento nell'applicazione e per l'osservanza del Regolamento (UE) 2016/679, in conformità all'art. 37 (Designazione del Responsabile della protezione dei dati), art. 38 (Posizione del Responsabile della protezione dei dati) e art. 39 (Compiti del Responsabile della protezione dei dati), dovrà, a titolo esemplificativo, espletare i seguenti compiti:

a) Progettazione ed attuazione del modello di Data Protection, in conformità al GDPR, nell'ambito di un programma di sicurezza delle informazioni e valutazione dei rischi.
b) Informazione, consulenza e indirizzo al Titolare e al Responsabili del Trattamento, nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal GDPR e dalle altre disposizioni legislative, provvedimenti e Linee Guida dell'Autorità Garante Privacy relative alla protezione dei dati.
c) Sorveglianza sull'osservanza del GDPR, delle altre normative relative alla protezione dei dati compresa la raccolta di informazioni per individuare i trattamenti svolti, l'analisi e la verifica dei trattamenti in termini di loro conformità.
d) Programmazione di un Piano Formativo che preveda formazione continua e sensibilizzazione per promuovere il rispetto della Privacy rivolto a tutti coloro che, ai sensi dell'art. 29 del richiamato Regolamento Europeo, trattano i dati sotto l'autorità del titolare del trattamento (dipendenti e non). A titolo esemplificativo: formazione giuridica in ambito di protezione dati personali, formazione tecnica in materia di sicurezza informatica, ecc.
e) Aggiornamento del Regolamento interno sulla protezione dei dati personali.

f) Analisi dell'impatto delle tecnologie utilizzate dalla Scuola in ambito di protezione dati e consulenza in merito alla Valutazione d'Impatto sulla protezione dei dati.
g) Cooperazione con il Garante Privacy per l'intermediazione tra le autorità di controllo e gli interessati.
h) Supporto e assistenza tecnico-giuridica ai competenti Uffici chiamati a predisporre la necessaria documentazione/modulistica in materia di trattamento dei dati personali (linee guida, disposizioni operative, modulistica e policy applicative relative alla protezione dei dati personali…).
i) Realizzazione di almeno 26 incontri in presenza, al fine di effettuare le attività elencate ai punti precedenti, le cui tematiche saranno:
   - Analisi e codifica dei dati Personali;
   - Attivazione e mantenimento del Registro delle attività di trattamento dei dati personali;
   - Attivazione e gestione del Registro dei Data Breach;
   - Attivazione del registro di segnalazioni e richieste di accesso ai dati personali;
   - Elaborazione di linee guida e di informative specifiche sul trattamento dei dati personali;
   - Aggiornamento di una procedura di gestione degli affidamenti di attività che comportano un trattamento a responsabili esterni, compresa la predisposizione delle specifiche clausole previste dall'articolo 28 del GDPR;
   - Elaborazione di procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento dei dati personali.

Sarà onere dell'incaricato garantire: controlli periodici on-site; la propria prestazione anche in orario pomeridiano e tempi di intervento, laddove necessario, entro le 24 ore lavorative dalla richiesta.

Art. 4 – Durata dell'incarico

L'incarico avrà durata di un anno a decorrere dalla data del conferimento dello stesso. È escluso il tacito rinnovo.

Art. 5 – Compenso

Il compenso previsto è pari ad € 650,00 (seicentocinquanta/00) omnicomprensivo delle ritenute previste per legge, e sarà corrisposto in un'unica soluzione ad incarico espletato.

Art. 6 – Modalità di presentazione dell'istanza

Gli aspiranti saranno selezionati, previa nomina di apposita commissione costituita da almeno n. 3 componenti, attraverso la comparazione dei curricula sulla base della valutazione dei titoli di cui alla tabella sottostante.

Criteri di valutazione	Punteggio
Laurea in aree disciplinari attinenti alle competenze professionali richieste	Punti 5/100
Partecipazione a master o corsi di specializzazione, comunque denominati, di durata non inferiore a 40 ore in materia di attuazione del GDPR.	Punti 10 per ogni corso/master Max. p 20/100
Possesso di certificazione in ambito di sicurezza informatica e delle informazioni (certificazioni ISO 27001 o BS7799 o UNI 11697:2017)	Punti 20
Esperienze lavorative come DPO	Punti 10 per ogni incarico annuale Max. p. 20/100
Esperienza documentata in ambito security/privacy	Punti 5 per ogni incarico annuale Max. p. 20/100
Qualità complessiva del progetto di gestione del servizio: utilizzo di standard, best practices e/o framework internazionali (es. ISO21500, PMI, Cobit5, ecc.)	Max. p. 15/100

Per manifestare il proprio interesse, gli aspiranti dovranno far pervenire all'ufficio protocollo, entro e non oltre il 26 gennaio 2019, alle ore 13.00, domanda indirizzata alla Dirigente scolastica corredata da proposta progettuale, curriculum vitae in formato europeo e griglia di autovalutazione come di seguito riportata.
I risultati della selezione saranno pubblicati all'albo dell'Istituto.

LA DIRIGENTE SCOLASTICA
prof.ssa Enza M. A. Santodirocco
Firma digitale (DPR 513/1997, art. 19)