MINISTERO DELL'ISTRUZIONE E DEL MERITO
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. Meccanografico**: FGIC83100Q – **Cod. Univoco**: UFJLON
Tel.: 0884 561316-568344 – **Sito web**: www.istitutogiovanni23.edu.it – **E-mail**: fgic83100q@istruzione.it-fgic83100q@pec.istruzione.it

Circ. n. 200

Monte Sant'Angelo, 4 giugno 2026

Al Personale Docente e Ata
Sede

Nel Sito web dell'Istituto:
- *Albo Online*
- *Circolari*
- *Amministrazione Trasparente*

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

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 (famiglia norme ISO 27000)
- Auditor di sistemi di gestione
- Esperti di Risk Management
- Consulenti/esperti sulle normative attinenti alla privacy e 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 (Knowledge):
   - Principi di privacy e protezione dei dati by design e by default
   - Diritti degli interessati previsti da leggi e regolamenti vigenti
   - 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
   - Metodologie di valutazione d'impatto sulla protezione dei dati e PIA
   - Norme tecniche ISO/IEC per la gestione dei dati personali
   - Tecniche crittografiche
   - Tecniche di anonimizzazione
   - Tecniche di pseudonimizzazione
   - Sistemi e tecniche di monitoraggio e "reporting"

- Strumenti di controllo per la produzione di documentazione
- Rischi critici per la gestione della sicurezza
- Tipici KPI (key performance indicators)
- Computer forensics (analisi criminologica di sistemi informativi)
- Politica di gestione della sicurezza e delle sue implicazioni con gli impegni verso gli utenti e i fornitori
- Best practices e standard nella analisi del rischio
- Best practices e standard nella gestione della sicurezza delle informazioni
- Norme legali applicabili ai contratti
- Nuove tecnologie emergenti
- Possibili minacce alla sicurezza
- Problematiche legate alla dimensione dei data set (es.: big data)
- Problematiche relative ai dati non strutturati (es: data analytics)
- Tecniche di attacco informatico e contromisure per evitarli

b) Abilità (Skill):
- Contribuire alla strategia per il trattamento e la protezione dei dati personali.
- Capacità di analisi, pianificazione, programmazione, organizzazione.
- Saper analizzare gli asset critici dell'Istituzione e identificare debolezze e vulnerabilità riguardo a 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 il rispetto della proprietà intellettuale (IPR) e delle norme della privacy.
- 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
- Governance dei sistemi informativi

d) Consolidata esperienza in ambito della sicurezza informatica (tecniche di attacco, crittografia, ecc.), dei 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 agli artt. 37 (Designazione del Responsabile della protezione dei dati), 38 (Posizione del Responsabile della protezione dei dati) e 39 (Compiti del Responsabile della protezione dei dati), dovrà, a titolo esemplificativo, espletare i seguenti compiti:

a) Progettazione e 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 Responsabile del Trattamento, nonché ai dipendenti che eseguono il trattamento – in merito agli obblighi derivanti dal GDPR e da altre disposizioni legislative, da provvedimenti e Linee Guida dell'Autorità Garante Privacy

relative alla protezione dei dati.

c) Sorveglianza sull'osservanza del GDPR e delle altre normative relative alla protezione dei dati, compresa la raccolta di informazioni per individuare e analizzare i trattamenti svolti al fine di verificarne la loro conformità.
d) Programmazione di un Piano formativo, teso a promuovere il rispetto della privacy, che preveda formazione continua e sensibilizzazione per 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 due incontri annuali, 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 comportino 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 e organizzative al fine di garantire la sicurezza del trattamento dei dati personali.

Sarà onere dell'incaricato garantire:
- controlli periodici on-site;
- 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 triennale a decorrere dal 26/09/2026. È escluso il tacito rinnovo.

Art. 5 – Compenso

Il compenso previsto è pari a 1.200,00 € (milleduecento/00 euro) omnicomprensivo delle ritenute previste per legge e sarà corrisposto in tre rate uguali al termine di ogni annualità.

Art. 6 – Modalità di presentazione e valutazione delle istanze

Gli aspiranti interessati dovranno far pervenire alla PEC istituzionale *fgic83100q@pec.istruzione.it*, entro e non oltre le ore 13.30 del 12 giugno 2026, istanza compilata secondo l'*All. 1* del presente avviso e corredata di proposta progettuale, curriculum vitae in formato europeo e griglia di valutazione di cui all'*All. 2*.

L'Istituzione, una volta pervenute le istanze di partecipazione alla selezione, previa nomina di apposita commissione costituita da almeno n. 3 componenti, procederà alla valutazione delle stesse sulla base dei criteri e mediante assegnazione dei punteggi indicati nella seguente tabella.

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 UNI 11697)	Punti 20
Esperienze lavorative come DPO	Punti 10 per ogni incarico annuale (*incarichi non cumulabili in uno stesso anno*) 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

I risultati della selezione saranno pubblicati all'albo dell'Istituto.

La Dirigente Scolastica
Prof.ssa Enza M. A. Santodirocco
Documento firmato digitalmente
(D.lgs. 82/2005 e norme correlate)

ALLEGATO 1

ISTANZA DI PARTECIPAZIONE ALL'AVVISO DI SELEZIONE – di cui alla Circ. interna n. 200/2026 – per il reclutamento di un Responsabile della Protezione dei Dati Personali (DPO) ai sensi dell'art. 37 del regolamento UE 2016/679

Alla Dirigente Scolastica
dell'I.C. "Giovanni XXIII"
Monte Sant'Angelo

Il/La sottoscritto/a _____, nato/a il ___/___/_____ a _____,

in servizio presso questo Istituto in qualità di _____,

C H I E D E

di poter svolgere l'**incarico triennale** di **Responsabile della Protezione dei Dati Personali (DPO) ai sensi dell'art. 37 del regolamento UE 2016/679**.

A tal fine, valendosi delle disposizioni di cui all'art. 46 del DPR 28/12/2000 n. 445, consapevole delle sanzioni stabilite per le false attestazioni e mendaci dichiarazioni, previste dal Codice Penale e dalle Leggi speciali in materia e preso atto delle tematiche proposte nei percorsi formativi,

D I C H I A R A

Sotto la propria responsabilità di:

- ☐ essere in possesso della cittadinanza italiana o di uno degli Stati membri dell'Unione europea;
- ☐ godere dei diritti civili e politici;
- ☐ non aver riportato condanne penali e di non essere destinatario di provvedimenti che riguardano l'applicazione di misure di prevenzione, di decisioni civili e di provvedimenti amministrativi iscritti nel casellario giudiziale ai sensi della vigente normativa;
- ☐ essere a conoscenza di non essere sottoposto a procedimenti penali;
- ☐ aver preso visione dell'Avviso emanato dall'I.C. "Giovanni XXIII" di Monte Sant'Angelo e di approvarne senza riserva ogni contenuto;
- ☐ essere in possesso dei requisiti di cui all'art. 2 dell'Avviso;
- ☐ essere disponibile a svolgere l'incarico senza riserva e secondo quanto previsto dall'Avviso;
- ☐ di non essere parente o affine entro il quarto grado del legale rappresentante dell'Istituto o di altro personale che ha preso parte alla predisposizione del bando di reclutamento.

A L L E G A

- ☐ **Curriculum Vitae in formato europeo**, riportante **solo i titoli e le esperienze valutabili** di cui all'art. 6 dell'Avviso;
- ☐ **Scheda di Auto/Etero-valutazione** – Allegato 2 dell'Avviso.

Monte Sant'Angelo, __/__/____ Firma

_____

ALLEGATO 2

SCHEDA DI AUTO/ETERO-VALUTAZIONE

Titoli/Esperienze valutabili	Punti	N. Titoli/ Esperienze	Tot. punti	Valutazione a cura della Commissione
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 UNI 11697)	Punti 20			
Esperienze lavorative come DPO	Punti 10 per ogni incarico annuale (*incarichi non cumulabili in uno stesso anno*) 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			

Monte Sant'Angelo, ___/___/_____ Firma

_____