MINISTERO DELL' ISTRUZIONE E DEL MERITO
Ufficio Scolastico Regionale per la Lombardia
Istituto Comprensivo Statale "Ai nostri caduti"
Via Pietro Nenni 2 - 20056 Trezzo sull'Adda (MI)
Scuola dell'Infanzia "G.Rodari" - Scuola Primaria "Ai nostri caduti" - Scuola Primaria "Don Gnocchi"
Scuola Secondaria di I° "P. Calamandrei"
Codice Fiscale: 91546630152 – Codice Meccanografico: MIIC8B2008 – Codice Univoco Ufficio: UFY1XJ
TEL.: 02.90933320 - MAIL: MIIC8B2008@istruzione.it - PEC: MIIC8B2008@pec.istruzione.it
Sito istituzionale: www.ictrezzo.edu.it
CANALE YOU TUBE: https://youtube.com/channel/UCMO3BV6dx52ruo_SpzPxwjA

CONTRATTO PER LO SVOLGIMENTO DELL'INCARICO TRIENNALE DI RESPONSABILE PROTEZIONE DATI (DPO/RPD) DI CUI ALL'ART. 37 DEL REGOLAMENTO UE 679/2016 E FORNITURA DEI SERVIZI PER L'ATTUAZIONE DELLA NORMATIVA IN MATERIA DI PRIVACY, TRASPARENZA, ACCESSIBILITÀ, DEMATERIALIZZAZIONE E LOTTA ALLA CORRUZIONE, AI SENSI DELL'ART. 36, COMMA 2, LETTERA A) DEL D.LGS. 50/2016. CIG. ZEA3AA2A10.

TRA

l'Istituto Comprensivo "AI Nostri Caduti" di Trezzo sull'Adda, rappresentato legalmente dalla Dott.ssa Patrizia Santini, Dirigente Scolastico pro-tempore, domiciliato per la sua carica presso l'Istituto Comprensivo "Ai Nostri Caduti" di Trezzo sull'Adda, Via Pietro Nenni 2, 20056 - Trezzo sull'Adda (MI)- C.F. 91546630152

E

la società Capital Security Srl con sede a Milano (MI), Via Monte Napoleone - P.IVA 10835430967, rappresentata dall'amministratore delegato Rossi Maurizio, si stipula il presente contratto di servizi per lo svolgimento delle funzioni di Data Protection Officer (responsabile della protezione dei dati), così come previsto dall'art 37 del Reg. UE 2016/679.

Il ruolo di Data Protection Officer è affidato al **Dott. Favero Giancarlo.**

1. Ruoli e compiti del Data Protection Officer

Il Dott. Favero Giancarlo, nominato Data Protection Officer svolgerà le seguenti attività:

1.1. Assunzione ruolo e responsabilità di Responsabile della Protezione dei Dati (RDP o "Data Protection Officer"), ai sensi ed in ottemperanza a quanto previsto dagli artt. 37, 38 e 39 del Regolamento Europeo.

Si prevede lo svolgimento delle seguenti attività:

- rispondere a tutti i quesiti posti da genitori, docenti, personale ATA, fornitori, collaboratori etc. sul Regolamento Europeo – GDPR e più in generale sulla sicurezza e privacy dei dati;

- rispondere a tutti i quesiti posti da genitori, docenti, personale ATA, fornitori, collaboratori etc. sul Regolamento Europeo – GDPR e più in generale sulla sicurezza e privacy dei dati;
- adempiere a quanto previsto dall'art. 37 comma 1 lettera a) del Regolamento UE che prevede l'obbligo di nomina del Responsabile della Protezione dei Dati ("Data Protection Officer");
- vigilare sull'operato di responsabili ed incaricati del trattamento relativamente alla corretta esecuzione delle istruzioni contenute in lettere di nomina, mansionari, regolamenti, disposizioni operative etc.;
- fornire pareri tecnico – legali in merito all'impatto che le nuove tecnologie (es. dati in cloud) e le nuove procedure operative avranno sulla protezione dei dati;
- affiancare il Titolare del trattamento (Dirigente Scolastico) ed il DSGA al fine di informarlo e fornire consulenza specialistica relativamente agli obblighi derivanti dal Regolamento UE, da successivi Codici di Comportamento e Schemi di Certificazione emessi dall'Autorità Garante;
- valutare la fondatezza e la liceità di richieste di accesso ai dati personali e di esercizio del diritto all'oblio esercitate dagli interessati;
- fornire supporto in fase ispettiva, qualora l'Istituto fosse oggetto di ispezione o verifica da parte dell'Autorità Garante per la Protezione dei Dati Personali, della Guardia di Finanza, della Polizia Postale o più in generale delle Autorità competenti;
- valutare se sussistano i presupposti per la notificazione di un evento di tipo "data breach"; se del caso, compilare il relativo modello e provvedere alla notificazione al Garante;
- eseguire la valutazione dei rischi inerenti al trattamento dei dati personali;
- supportare il Dirigente Scolastico nella compilazione del Registro delle violazioni dei dati e degli incidenti informatici;
- aggiornare laddove necessario i Registri delle attività di trattamento;
- informare il Dirigente Scolastico ed i referenti circa le previsioni normative e le procedure da adottare per non incorrere nelle violazioni e nelle conseguenti sanzioni.

1.2. Mantenimento e aggiornamento gestione degli adempimenti previsti da GDPR – Regolamento Europeo 2016/679 e del D.Lgs. 196/2003, così come modificato dal D.Lgs. 101/2018

Si prevede lo svolgimento delle seguenti attività:

- ricognizione della situazione attuale in termini di:
  - struttura organizzativa
  - banche dati trattate
  - architettura hardware e software
- predisposizione/aggiornamento del Registro dei trattamenti
- data Protection Impact Assessment, comprensivo di analisi dei rischi relativi a:
  - aspetti legali, normativi e organizzativi
  - luoghi fisici
  - risorse hardware

  - risorse logiche
  - accessi ad Internet
  - risorse dati (cartacei ed elettronici)
  - trattamenti effettuati mediante architetture in cloud
- individuazione delle misure di sicurezza
  - stesura del piano di attuazione delle misure di sicurezza
- revisione processi, sistemi e modulistica in ottica di Privacy by Design e Privacy by Default
- predisposizione nuove informative
- predisposizione lettere di nomina per le varie figure previste dal GDPR e quelle ritenute comunque necessarie a fronte di analisi dei rischi e registro dei trattamenti (Titolare, Responsabile, Incaricato, Custode delle Password, Amministratore di Sistema, Azienda esterna, Consulenti o collaboratori esterni)
- predisposizione procedure operative:
  - riscontro all'interessato
  - gestione delle password
  - profilazione degli utenti
  - smaltimento e riutilizzo dei supporti di memorizzazione e strumenti elettronici
  - gestione del salvataggio e ripristino dei dati
  - altre procedure operative
- predisposizione/aggiornamento del Regolamento per il corretto utilizzo degli strumenti informatici e telematici
- predisposizione/aggiornamento del Regolamento per lo smaltimento e il riutilizzo degli strumenti elettronici e dei supporti di memorizzazione.

1.3. Monitoraggio continuo del livello di sicurezza mediante modelli MMS e KPI (Indicatori Chiave di Performance)

Il servizio dura 12 mesi e prevede il monitoraggio continuo del livello di sicurezza mediante analisi dei modelli MMS (Modello per il Monitoraggio della Sicurezza) su base periodica, l'individuazione e gestione di casistiche significative in termini ad esempio di frequenza e gravità, e il calcolo periodico di indicatori chiave di performance, come ad esempio il livello di sicurezza, il numero di violazioni dei dati, il numero di incidenti informatici, il numero di sanzioni comminate etc.

1.4. Verifica annuale da remoto con DS e DSGA per valutare il livello di adeguamento al GDPR, l'individuazione di aree di scopertura e criticità, e la loro risoluzione

Al fine di accompagnare ed affiancare il DS, il DSGA ed il Personale Amministrativo e tecnico nel percorso di adeguamento al GDPR, si ritiene utile effettuare con cadenza annuale un incontro, finalizzato a valutare il livello di adeguamento al GDPR e l'individuazione di eventuali aree di scopertura o di criticità. Alla fine dell'incontro il DPO predisporrà un verbale delle verifiche effettuate e delle azioni da mettere in atto.

1.5. Settantadue scansioni di vulnerabilità su sito web e su registro elettronico

Il servizio prevede l'esecuzione di due scansioni di vulnerabilità al mese, una sul sito web istituzionale e una sul registro elettronico, al fine di individuare vulnerabilità e configurazioni poco sicure.

Alla fine delle scansioni di vulnerabilità, nel caso vengano riscontrate vulnerabilità gravi oppure il livello di rischio medio sia pari a 4 oppure 5, verranno inviati all'Istituto i report dettagliati prodotti dalla piattaforma di vulnerability assessment, contenenti la descrizione dettagliata delle vulnerabilità riscontrate e le attività da svolgere per la loro risoluzione.

2. Corsi di formazione specialistica

2.1. Formazione centralizzata in presenza al personale di Segreteria, DS e DSGA

Si prevede di tenere una sessione all'anno di formazione in presenza, presso l'I.C. Basiano, oppure a distanza, per DS, DSGA e personale di segreteria, eventuale personale tecnico ed eventuali Funzioni Strumentali, della durata media di circa due ore.
Il taglio dell'intervento è molto interattivo e pratico, mantenendo al minimo l'esposizione della teoria e privilegiando l'esposizione di casi pratici e dando adeguato spazio alle importanti domande dei partecipanti.
I corsi sono tenuti da relatori di adeguata seniority e standing, con profonda conoscenza della materia, in grado quindi di rispondere con precisione e cognizione di causa a qualsiasi quesito venga posto.
Alla fine dell'intervento può venire rilasciato un regolare attestato di partecipazione, unitamente ad una relazione con l'esplicitazione di indicatori quantitativi e qualitativi di gradimento.

2.2. Formazione centralizzata tramite internet al personale docente

Si prevede inoltre di tenere ogni anno una sessione di formazione annuale interattiva a distanza tramite internet, della durata di circa un'ora e mezza, dedicata al personale docente, per ciascun Istituto aderente all'offerta in rete. La sessione è interattiva con audio e video bidirezionale, quindi i partecipanti avranno la possibilità di porre domande al relatore e di avere le risposte in tempo reale. Le date della sessione di formazione saranno concordate e comunicate con adeguato anticipo. In alternativa od oltre a quanto appena riportato, è possibile mettere a disposizione una registrazione della sessione, comprensiva di slideshow e commento audio e video registrato, che ciascun docente potrà seguire in maniera autonoma e indipendente.

2.3. Possibilità di videoriprendere l'esposizione del relatore

Nel caso l'Istituto lo ritenesse utile, viene data la possibilità al personale dell'Istituto di effettuare riprese filmiche (con risorse proprie dell'Istituto, come ad esempio videocamere, smartphone etc.) l'incontro formativo centralizzato in presenza, in modo da poter permettere anche a chi era assente o impossibilitato a partecipare, di rivedere il corso e di maturare quindi una certa conoscenza delle problematiche trattate.

2.4. Trenta Ticket per quesiti successivi

Si ha la possibilità di porre quesiti di qualsiasi tipo, ai quali viene data risposta in forma scritta nel tempo massimo di tre giorni lavorativi.

Nel costo dell'intervento formativo sono inclusi trenta Ticket.

2.5. Programma del corso

Fermo restando il taglio fortemente interattivo dell'intervento e lo spazio lasciato alle domande poste dai partecipanti, si prevede di seguire il seguente programma:

- Perché il nuovo Regolamento Europeo
- Come "lavora" il nuovo Regolamento: differenze con l'attuale quadro normativo
- Il principio di responsabilizzazione
- La figura del data protection officer
- Il registro dei trattamenti
- Il privacy impact assessment
- Protection by design e protection by default
- L'obbligo di notificazione del data breach
- Le misure di sicurezza
- I codici di condotta e le certificazioni
- Il quadro sanzionatorio.

3. Garanzia assicurativa con massimale fino a 8.000,00 Euro in caso di sanzioni comminate dal Garante per la protezione dei dati personali, per violazione del GDPR o del D.Lgs. 196/2003.

Il servizio prevede una garanzia assicurativa (erogata sotto forma di penale) con massimale fino a 8.000,00 Euro in caso di sanzioni comminate dal Garante per la protezione dei dati personali per violazione del GDPR o del D.Lgs. 196/2003.

4. Durata dell'incarico

Il presente incarico deve intendersi valido per tre anni dalla data del 27 Aprile 2023 fino al 26 Aprile 2026.

5. Risoluzione dell'incarico

La clausola di salvaguardia del presente contratto triennale prevede la possibilità di recesso annuale da parte dell'istituto senza necessità di motivazione mediante una semplice comunicazione via PEC. Il Committente potrà procedere in qualsiasi momento dell'anno alla revoca dell'incarico conferito mediante comunicazione da inviare via PEC, con pagamento del corrispettivo in base allo stato di avanzamento del lavoro.

Anche il DPO potrà recedere dal contratto dandone comunicazione mediante lettera raccomandata A/R, in tal caso il committente non sarà tenuto al pagamento del lavoro svolto fino a quel momento.

Qualora fosse accertato il difetto del possesso dei requisiti prescritti si procederà alla risoluzione del contratto e sarà liquidato il corrispettivo pattuito solo con riferimento alle prestazioni già eseguite e nei limiti dell'utilità ricevuta.

Il contratto sarà sottoposto a condizione risolutiva nel caso di sopravvenuta disponibilità di una convenzione Consip S.p.A. avente ad oggetto servizi *[o forniture]* comparabili con quelli oggetto di affidamento, ai sensi della norma sopra citata;

6. Determinazione del compenso

Il compenso annuale spettante per l'espletamento delle prestazioni stabilite nel presente incarico ammonta a **€ 450,00 + IVA 22%,** per un totale triennale di **€ 1.350,00 + IVA 22%.**

7. Modalità di pagamento

Il pagamento del corrispettivo stabilito verrà liquidato a seguito di ricevimento di regolare fattura elettronica, all'atto dell'accettazione dell'incarico da parte del DPO, entro 30 giorni dal ricevimento della stessa. Codice Univoco dell'Ufficio: UFY1XJ.

Prima di procedere al saldo delle fatture l'Istituto verificherà la regolarità contributiva (DURC), il possesso dei requisiti previsti dall'art. 80 del D. Lgs. n. 50/2016 e l'adempimento della comunicazione relativa agli obblighi di tracciabilità dei flussi finanziari previsti dalla legge del 13 agosto 2010, n. 136 («Piano straordinario contro le mafie, nonché delega al Governo in materia di normativa antimafia») e dal D.L. del 12 novembre 2010, n. 187 («Misure urgenti in materia di sicurezza»), convertito con modificazioni dalla legge del 17 dicembre 2010, n. 217, e relative modifiche, integrazioni e provvedimenti di attuazione.

8. Tutela della segretezza

Tutti i dati, le informazioni e i documenti esaminati e gestiti dal DPO e dalla sua organizzazione nello svolgimento dell'incarico professionale devono essere considerati riservati. Pertanto, è fatto assoluto divieto di divulgazione o comunicazione.

9. Trattamento dati personali

Il fornitore nel trattamento dei dati di cui venga a conoscenza nello svolgimento della fornitura oggetto del presente ordine, si impegna ad osservare ed a far osservare ai propri dipendenti e collaboratori, le disposizioni di legge vigenti a livello nazionale ed europeo e quanto stabilito negli accordi che governano il rapporto.

10. Foro competente

Per ogni controversia relativa al presente contratto si elegge competente il Foro di Milano.

11. Norme di rinvio

Non essendo soggetto a registrazione obbligatoria, il presente contratto verrà registrato solo in caso d'uso, a cura e spese della parte che vi abbia interesse.

Trezzo sull'Adda, 27 Aprile 2023
Letto, approvato e sottoscritto

CAPITAL SECURITY
Il legale rappresentante
Dott. Maurizio Rossi

IL DIRIGENTE SCOLASTICO
Dott.ssa Patrizia Santini
(1)Documento firmato digitalmente ai sensi del Codice dell'Amministrazione Digitale e normativa connessa)