MINISTERO DELL'ISTRUZIONE, DELL'UNIVERSITA' E DELLA RICERCA
UFFICIO SCOLASTICO REGIONALE DELLA LOMBARDIA
ISTITUTO COMPRENSIVO DI SCUOLE PRIMARIE E SECONDARIE DI PRIMO GRADO
"TEODORO CIRESOLA"
V.LE BRIANZA N. 14/18 e VIA VENINI N. 80 - 20127 MILANO (MI) - Tel. 02/88444661 – Fax 02/88444665
COD. MECC. MIIC81700R – COD. FISC. 97117370151 - e-mail: MIIC81700R@istruzione.it -
MIIC81700R@pec.istruzione.it - www.icsciresola.gov.it

Prot. n. 2685/C14 Milano, 24/05/2018

CIG Z4923B9D11

Contratto per **l'adeguamento ai requisisti richiesti dal Regolamento UE 679/2016 (G.D.P.R) in materia di protezione dei dati personali e conferimento incarico DPO/RPD (Data Protection Officer / Responsabile della Protezione dei dati)**

Tra

L'Istituto Comprensivo di Ciresola (MI), rappresentato dalla Dott.ssa Anna Polliani Dirigente Scolastico, nata a Milano il 25/07/1970 COD. FISC. PLLNNA70L65F205K e domiciliato per la sua carica presso Istituto Comprensivo di Ciresola (MI) codice fiscale 97117370151

E

Privacycert Lombardia S.r.l. con sede legale in Bergamo, via Passaggio Don Seghezzi, 2 – Bergamo, 24122, P. IVA.: 04224740169
nella persona del suo legale rappresentante il sig. Zampetti Massimo nato a Bergamo (BG) il 02/10/1988, residente in Bergamo via Borgo Palazzo, 142, COD. FISC.: ZMPMSM88R02A794T.

1. INTRODUZIONE: Le novità del Regolamento UE

Il Regolamento Generale sulla Protezione dei Dati (GDPR) è la nuova normativa europea che armonizza e supera le normative attualmente vigenti negli Stati facenti parte della Comunità Europea, **punta a rafforzare e proteggere da minacce presenti e future i diritti alla protezione dei dati personali dei propri cittadini**, dentro e fuori dall'Unione Europea.
Per farlo il **GDPR** introduce nuovi **obblighi** e nuove **sanzioni** che impongono agli Enti l'adozione di specifiche misure sulla protezione dei dati personali.
Tra gli elementi introdotti dalla normativa ci sono: la necessità di gestire un registro dei trattamenti e garantire nel tempo la sicurezza dei dati; l'obbligo di notificare i data breach; l'esigenza di introdurre la figura del **Data Protection Officer**; l'esigenza di adottare un approccio ispirato al principio di "*privacy design;* l'inasprimento delle **sanzioni**.

2. OBIETTIVO

Sviluppare un sistema gestionale che consenta di identificare e attuare quanto necessario per rispondere agli obblighi giuridici relativi al Regolamento UE 679/2016 (G.D.P.R.) in materia di protezione dei dati personali e conferire incarico **DPO**.

3. MODALITA' OPERATIVE

Si definirà con Voi un calendario operativo che prevede sia attività presso la vostra organizzazione che attività di back office. In via orientativa le attività si svolgeranno come segue:
Modulo 1: entro 10 giorni dalla sottoscrizione del contratto, o dall'affidamento dell'Incarico.

Modulo 2: entro 25 giorni dalla sottoscrizione del contratto, o dall'affidamento dell'Incarico.
Modulo 3: entro 35 giorni dalla sottoscrizione del contratto, o dall'affidamento dell'Incarico.

Si sottolinea che tutte le informazioni e i dati che entreranno in nostro possesso verranno considerati riservati e non saranno divulgati in nessun modo e per alcun motivo se non dietro Vostra specifica autorizzazione.

4. STRUTTURAZIONE DELL'INTERVENTO

MODULO 1 – entro 10 gg
Il primo passo consiste **nell'analisi dell'organizzazione** e del livello di adempimento normativo acquisito tramite:

- Attività di audit presso la sede della Scuola in cui il Dato personale viene trattato quotidianamente, o in remoto;
- Definizione del contesto in cui opera l'Istituto Scolastico;
- Politiche adottate per la sicurezza dei dati personali;
- Gestione delle risorse.

Contestualmente si procederà alla **preliminare verifica** dell'applicazione dei requisiti al Regolamento UE 679/2016 (G.D.P.R.) all'interno dell'Istituto Scolastico.

MODULO 2 – entro 25 gg
La seconda fase consente di impostare in modo chiaro le **azioni necessarie** per conseguire la conformità legislativa attraverso:

- Valutazione dei rischi legati alla sicurezza dei dati personali;
- Trattamento del rischio relativo alla sicurezza dei dati personali;
- Assegnazione di ruoli compiti e responsabilità;
- Obiettivi per la sicurezza dei dati personali e pianificazione per conseguirli;
- Misura delle prestazioni;
- Affinità con altre norme internazionali (ISO 27001, BS 10012).

MODULO 3 – entro 35 gg
Tutto quanto sopra descritto prevederà lo sviluppo e la consegna di una parte documentale (**Sistema Gestionale**) costituita da:

- Manuale;
- Procedure;
- Istruzioni;
- Politiche
- Modulistica.

Il servizio prevederà una parte gestita in **forma cartacea** (istruzioni, politiche e procedure) e una **parte digitale** (registri, modelli di nomina e lettere di incarico, Valutazione del rischio etc.) appositamente dedicata in un'area riservata.

5. MODALITA' DI REALIZZAZIONE DEL PROGETTO

5.1
PROGETTAZIONE del Sistema di gestione per la sicurezza dei dati personali
Il sistema aviene progettato avendo come riferimento i principi di:

- BS 10012:2017 Data Protection - Sistemi di gestione per la sicurezza delle informazioni personali;
- ISO 27001:2013 Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni;

5.2
ELABORAZIONE della documentazione del Sistema
La parte documentale verrà sviluppata elaborando procedure che consentano la:

- Definizione del contesto in cui opera l'organizzazione;
- Politiche adottate per la sicurezza dei dati personali;
- Valutazione dei rischi legati alla sicurezza dei dati personali;
- Trattamento del rischio relativo alla sicurezza dei dati personali;
- Assegnazione di ruoli compiti e responsabilità
- Gestione delle risorse;
- Obiettivi per la sicurezza dei dati personali e pianificazione per conseguirli;
- Misura delle prestazioni;

5.3
IMPLEMENTAZIONE e VERIFICHE del Sistema di gestione della Sicurezza dei dati personali.
In questa fase la Direzione dovrà definire ed **assegnare** in modo formale e documentato **responsabilità** ed autorità a tutte le figure coinvolte nella gestione e nella attuazione del Sistema di gestione per la sicurezza dei dati personali.

Le verifiche (nel numero di minimo 2 audit nella durata del contratto) **rappresentano tutte le attività di controllo periodico**, da effettuare in sede e/o remoto, finalizzate all'accertamento dell'efficacia del sistema stesso ed alla individuazione di eventuali azioni correttive e/o preventive.

6. CONFERIMENTO INCARICO DPO/RPD

Tra gli elementi introdotti dalla normativa viene individuata l'esigenza di introdurre la figura del **Data Protection Officer** e la nostra organizzazione, grazie alla propria competenza e professionalità, possiede i necessari requisiti per poter ricoprire tale ruolo.

Compito del **DPO**, così come previsto dal Regolamento è:

- ✓ **informare e fornire consulenza (telefonica o digitale)** al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento;

- ✓ **sorvegliare l'osservanza del presente regolamento**, di altre disposizioni dell'Unione o degli Stati membri relative alla **protezione dei dati** nonché delle politiche del titolare del trattamento o del responsabile del trattamento in materia di protezione dei dati personali, compresi l'attribuzione delle responsabilità, la sensibilizzazione e la **formazione del personale** (quattro ore complessive suddivise in due ore via webinar, e due ore in aula magna) che partecipa ai trattamenti e alle connesse attività di controllo;

- ✓ **fornire, se richiesto, un parere in merito alla valutazione d'impatto** sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35 del Regolamento;

- ✓ **cooperare con l'autorità di controllo**;

- ✓ **fungere da punto di contatto per l'autorità di controllo** per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36 del Regolamento, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione.

Il conferimento di incarico, la sua accettazione e le modalità di trasmissione dei dati all'Autorità di Controllo (Garante della Privacy) avverranno con **modulistica ufficialmente** proposta dal **Garante** stesso.

7. DURATA CONFERIMENTO INCARICO DPO

Il presente incarico di "*Data Protection Officer*" ha la **durata di anni 1 (uno)** dalla sua sottoscrizione.

8. COSTI DEI SERVIZI RESI

Gli importi, al netto dell'IVA, per le attività ed i servizi di cui alla presente proposta sono:

- **€ 1.300,00: adeguamento GDPR 679/2016, incarico di DPO** in conformità ai sensi degli artt. 37-39 GDPR e svolgimento di tutte le attività ad esso collegate **e tutte le attività correlate (**non sono previste spese di trasferta alla sede in indirizzo indicata né altri costi accessori).

L'importo complessivo è quindi pari ad **€ 1.300,00 oltre IVA (22%).**

N.B. Non sono compresi costi per servizi diversi da quelli descritti nel presente documento. (Esempio: interventi sui dispositivi elettronici, sistemi di protezione informatici, certificazioni, ecc..).

9. MODALITÀ' DI PAGAMENTO

Gli importi, al netto dell'IVA, per le attività ed i servizi di cui alla presente proposta sono:

n. 1 rata da **€ 1.300,00** + IVA entro 30 giorni data fattura (la fattura verrà emessa alla consegna dei documenti)

Gli importi suddetti verranno regolati attraverso emissione di regolare fattura elettronica e il pagamento verrà effettuato mediante Bonifico Bancario intestato a Privacycert Lombardia S.r.l.:
Codice IBAN: IT77 C031 1111 1010 0000 0001 619
Unione di Banche Italiane SpA, Piazza Vittorio Veneto 8, Bergamo.

10. OBBLIGHI DI RISERVATEZZA

Le parti si obbligano a mantenere riservati i dati e le informazioni, ivi comprese quelle che transitano per le apparecchiature di elaborazione e di trasmissione dati, di cui vengano in possesso e, comunque, a conoscenza, a non divulgarli in alcun modo e in qualsiasi forma e a non farne oggetto di utilizzazione a qualsiasi titolo per scopi diversi da quelli strettamente necessari all'esecuzione del presente contratto.

11. FORZA MAGGIORE

Le Parti non potranno essere considerate responsabili per ritardi o mancata esecuzione di quanto stabilito nel contratto, qualora ciò sia dipeso esclusivamente da eventi al di fuori della sfera di controllo della Parte e la Parte non adempiente abbia agito con il massimo impegno per prevenire i suddetti eventi e/o risolverne le conseguenze. L'onere di provare che il verificarsi di tali eventi impedisce la tempestiva esecuzione, o l'esecuzione stessa, grava sulla parte inadempiente. La Parte che abbia avuto notizia di un evento che possa considerarsi di forza maggiore ne darà immediata comunicazione all'altra e le Parti si incontreranno immediatamente al fine di concordare insieme gli eventuali rimedi per ripristinare quanto prima la normale funzionalità dei servizi.

12. RISOLUZIONE E RECESSO DEL CONTRATTO

Diffida ad adempiere
Di fronte all'inadempimento di una parte, l'altra parte potrà intimare per iscritto, mediante una comunicazione non generica corredata di adeguata documentazione tecnica, di porre rimedio a tale inadempimento entro il termine di 30 giorni, avvertendo esplicitamente la controparte che, decorso inutilmente tale termine, la parte

intimante potrà dichiarare per iscritto la risoluzione del contratto o della sola parte cui è relativo l'inadempimento.

Clausola risolutiva espressa
Il contratto si risolverà di diritto ai sensi dell'art. 1456 c.c. quando l'inadempienza riguardi una delle seguenti obbligazioni:
- *mancata esecuzione delle obbligazioni di risultato di cui ai punti 2-3-4-5-6 del presento contratto;*
- *caso di subappalto non autorizzato;*
- *mancato pagamento dei corrispettivi al Fornitore oltre 30 giorni;*
- *violazione del segreto aziendale e della riservatezza di cui all'art. 10 del presente contratto;*
- *violazione tutela della proprietà intellettuale*.

Recesso del contratto
Il cliente può recedere dal presente contratto dando un preavviso di 30 gg a mezzo PEC o r.a.r. In tal caso il cliente pagherà comunque l'importo della rata relativa alla fase in corso.

13. FORO COMPETENTE

Per qualsiasi controversia, sarà competente esclusivamente il Foro di Bergamo.

PrivacyCert Lombardia S.r.l.

……
Timbro

La Dirigente scolastica
Dott.ssa Anna Polliani
Documentazione firmata digitalmente
ai sensi del C.A.D. e normativa connessa
……
Timbro

Ai sensi e per gli effetti degli art. 1341 e 1342 cc, il cliente approva specificamente le seguenti clausole: 5. Modalità di realizzazione del progetto; 6. Incarico di DPO; 7. Durata conferimento incarico DPO; 8. Costi dei servizi resi; 9. Modalità di Pagamento; 10. Obblighi di riservatezza; 11. Forza maggiore; 12. Risoluzione e recesso del contratto; 13. Foro competente.

La Dirigente scolastica
Dott.ssa Anna Pollian
Documentazione firmata digitalmente
ai sensi del C.A.D. e normativa connessa

……

Timbro

PrivacyCert Lombardia S.r.l.

……

Timbro

Il trattamento dei dati che La riguardano viene svolto nell'ambito della banca dati di PrivacyCert Lombardia S.r.l. e nel rispetto di quanto stabilito ai sensi e per gli effetti dell'art. 13 del D. Lgs. 196/2003. Il trattamento dei dati è effettuato per finalità gestionali, statistiche, promozionali e commerciali dei nostri servizi. Ella potrà richiedere in qualsiasi momento la modifica o la cancellazione dei dati scrivendo a: PRIVACYCERT LOMBARDIA SRL, Passaggio Don Seghezzi, 2 – Bergamo, 24122

La Dirigente scolastica
Dott.ssa Anna Polliani
Documentazione firmata digitalmente
ai sensi del C.A.D. e normativa connessa

PrivacyCert Lombardia S.r.l.

……

Timbro

……

Timbro