**CONTRATTO DI NOMINA DEL RESPONSABILE DEL TRATTAMENTO DEI DATI AI SENSI E PER GLI EFFETTI DELL'ART. 28 DEL REGOLAMENTO EUROPEO 27 APRILE 2016, N. 679 (GDPR) E DELL'ART. 2 QUATERDECIES DEL D. LGS. 196/2003 E SS.MM. II.**

**TRA**

Istituto Comprensivo di Volpago del Montello (P. IVA 02683390401), in persona del suo Rappresentante legale *pro tempore*, con sede in Via Francesco Maria Preti, 1 - 31040 Volpago del Montello (TV),

(*Titolare del trattamento/Titolare*)

**E**

A.R. STUDIO WEB DI ANDREA ROSSI (P.IVA 02683390401), in persona del suo legale rappresentante *pro tempore*, con sede/domiciliato in VIA SAN PIO X 6/3 - 31040 Volpago del Montello (TV) - Italia,

(*Responsabile del trattamento/Responsabile*)

**premesso che:**

- Il titolare del trattamento di dati personali può proporre una persona fisica, una persona giuridica, una pubblica amministrazione e qualsiasi altro ente, associazione od organismo quale responsabile al trattamento dei dati che sia nominato tra soggetti che per esperienza, capacità ed affidabilità forniscano idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento di dati personali, ivi compreso il profilo di sicurezza;
- il responsabile del trattamento deve inoltre presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti della normativa richiesti dalle disposizioni *pro tempore* vigenti in materia e, altresì, garantisca la tutela dei diritti dell'interessato;
- il responsabile deve procedere al trattamento secondo le istruzioni impartite dal titolare per iscritto, mediante il presente contratto e/o con eventuali accordi successivi;
- è intenzione del titolare consentire l'accesso sia al responsabile che alle persone autorizzate al trattamento per i soli dati personali la cui conoscenza è necessaria per adempiere ai compiti loro attribuiti;
- Istituto Comprensivo di Volpago del Montello è titolare del trattamento di dati personali;
- A.R. STUDIO WEB DI ANDREA ROSSI svolge per Istituto Comprensivo di Volpago del Montello la funzione di Amministratore di Sistema, ai sensi del contratto in essere tra le parti, stipulato in data 18/07/2023;
- sussistono in capo a A.R. STUDIO WEB DI ANDREA ROSSI i requisiti su detti, imposti dall'art.28 GDPR.

In virtù di quanto sopra premesso, che costituisce parte integrante del presente accordo, Istituto Comprensivo di Volpago del Montello

**nomina**

A.R. STUDIO WEB DI ANDREA ROSSI *"responsabile del trattamento"*
ai sensi e agli effetti dell'art. 28 GDPR per i trattamenti di tutti i dati personali realizzati nell'ambito dell'incarico conferito.
In tale qualità A.R. STUDIO WEB DI ANDREA ROSSI è tenuto/a al rispetto delle disposizioni di Legge e di Regolamento in materia di tutela dei dati personali.
In particolare è tenuto a osservare le disposizioni che seguono:

**1. DESCRIZIONE DEL TRATTAMENTO DEL RESPONSABILE**

Il Responsabile è autorizzato a trattare, per conto del Titolare del trattamento, i dati personali necessari per fornire i servizi oggetto del contratto in essere tra le parti, che costituisce il presupposto necessario del presente.

**2. OBBLIGHI DEL RESPONSABILE IN QUALITA' DI AMMINISTRATORE DI SISTEMA**

2.1 Attivare le credenziali di autenticazione ai soggetti incaricati del trattamento, su espressa indicazione del Titolare del trattamento dei dati personali, per tutti i trattamenti che vengano effettuati con l'utilizzo di strumenti informatici, nonché assumere il compito di gestire a livello informatico tutti i soggetti incaricati del trattamento.
2.2 Individuare le politiche che dovranno essere adottate per garantire la massima protezione dei sistemi contro i virus informatici e verificarne l'efficacia ogni tre mesi. Inoltre, egli dovrà assicurare e gestire adeguati sistemi di salvataggio e di ripristino dei dati (backup/recovery) anche automatici.
2.3 Proteggere gli elaboratori dal rischio di accesso da parte di personale interno privo di autorizzazione nonché da parte di soggetti esterni.
2.4 Garantire la sicurezza dei dati sensibili o giudiziari contro l'accesso da parte di chiunque abusivamente si introduca nel sistema informatico o telematico.
2.5 Predisporre sistemi idonei alla registrazione degli accessi logici (autenticazione informatica) ai sistemi di elaborazione e agli archivi elettronici da parte sua (nella sua qualità di amministratore di sistema); tali registrazioni (access log) devono avere caratteristiche di completezza, inalterabilità e possibilità di verifica della loro integrità adeguate al raggiungimento dello scopo di verifica per cui sono richieste.
2.6 Dare tempestiva comunicazione al Titolare del trattamento dei dati personali qualora vengano rilevati rischi relativamente alle misure di sicurezza predisposte per la protezione dei dati trattati.
2.7 Coordinare assieme al Titolare le attività operative degli autorizzati al trattamento nello svolgimento delle mansioni loro affidate per garantire un corretto, lecito e sicuro trattamento delle informazioni nell'ambito del sistema informatico.
2.8 Collaborare con il Titolare per l'attuazione delle prescrizioni impartite dal Garante.
2.9 Verificare il rispetto delle norme sulla tutela del diritto d'autore sui programmi installati negli elaboratori presenti nelle strutture dell'Istituto.
2.10 Comunicare i nominativi della persona o delle persone che saranno assegnate a questo Istituto per l'espletamento del Vostro incarico ed aggiornare tempestivamente lo stesso qualora ci siano delle modifiche nell'assegnazione.

**3. NOMINA DI ULTERIORE RESPONSABILE ESTERNO DEL TRATTAMENTO (O SUB RESPONSABILE)**

3.1 Il Titolare del trattamento deve autorizzare a sub-delegare ad altro Responsabile trattamenti di dati demandati in forza del contratto tra le parti.
A tale autorizzazione segue l'atto di nomina del sub-responsabile che deve essere inoltrato dal Responsabile al Titolare.
3.2 Parimenti, il Responsabile informa il Titolare anche di eventuali modifiche riguardanti l'aggiunta o la sostituzione di altri responsabili, così da permettergli di esercitare il diritto di opporsi.
3.3 Spetta in capo al Responsabile del trattamento l'obbligo di assicurarsi che il sub-responsabile presenti le garanzie sufficienti per quanto riguarda l'adozione delle misure tecniche e organizzative necessarie affinché il trattamento dei dati sia conforme alle esigenze del GDPR. Se il sub-responsabile non rispetta gli obblighi in materia di protezione dei dati personali, il Responsabile risponde solidalmente nei confronti del Titolare del trattamento.

**4. VERIFICHE PERIODICHE/ AUDIT**

4.1 Il Responsabile esterno deve fornire la massima disponibilità e collaborazione, consentendo, se necessario, l'accesso ai propri locali, nonché la verifica delle procedure applicate nella gestione dei documenti cartacei ed elettronici affinché Titolare possa svolgere, anche tramite consulenti ed addetti di propria fiducia, le "verifiche periodiche" previste dall'art. 28 GDPR, necessarie per accertarsi del rispetto degli obblighi di questo accordo e della normativa sopra citata.
4.2 Il Responsabile riferisce per iscritto al Titolare, sui dettagli relativi all'adempimento di quanto disposto dalla Legge e dal presente atto di nomina, ogni qualvolta quest'ultimo ne faccia richiesta.

**5. GESTIONE MODULISTICA PRIVACY**

5.1 Il Responsabile esterno deve operare in maniera conforme ai principi di efficienza e trasparenza, tramite adeguate procedure e garantendo la custodia, la non alterazione e l'agevole reperimento della documentazione relativa agli adempimenti formali prescritti dalla normativa.
5.2 Il Responsabile esterno, su richiesta del Titolare, deve coadiuvare quest'ultimo nella difesa in caso di procedimenti dinanzi al Garante per la protezione dei dati personali o all'Autorità giudiziaria ordinaria anche consentendogli la tempestiva esibizione della modulistica privacy e dei documenti probatori rientranti nella competenza del Responsabile stesso.

**6. CESSAZIONE DEL RAPPORTO**

All'atto della cessazione, per qualsiasi causa, delle operazioni di trattamento da parte del Responsabile, quest'ultimo restituisce tempestivamente al Titolare, salvo comprovati obblighi di legge, e comunque entro un mese dalla cessazione, i dati personali oggetto delle operazioni di trattamento, su qualunque supporto detenuto (cartaceo o informatico, originali e copie), rilasciando contestualmente un'attestazione scritta che presso la propria struttura non ne esista alcuna ulteriore copia.

**7. DURATA**

7.1 Il presente atto ha la durata del rapporto tra le parti, salvo cessazione o esercizio del diritto di revoca da parte del titolare.
7.2 Lo stesso sarà rinnovato di diritto in caso di rinnovo del contratto principale.

**8. REVOCA**

Il Titolare ha facoltà di revocare il presente mandato nel caso di reiterate violazione GDPR con effetto immediato, previa notifica scritta allo stesso via PEC e senza che nulla sia ulteriormente dovuto.

**9. LEGGE APPLICABILE E FORO COMPETENTE**

Il presente contratto è disciplinato secondo la Legge Italiana. Per quanto ivi non esplicitamente previsto si applicheranno le norme del Codice Civile nonché le altre norme giuridiche inderogabili aventi efficacia di legge.
Tutte le controversie derivanti dal presente contratto, comprese quelle relative alla sua validità, interpretazione, esecuzione e risoluzione, saranno di competenza esclusiva del Foro già individuato nel contratto principale.
Volpago del Montello, 18/07/2023

Istituto Comprensivo di Volpago del Montello
Firma

_____

A.R. STUDIO WEB DI ANDREA ROSSI
Firma

_____

**ALLEGATO A - MISURE DI SICUREZZA**

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il Responsabile del trattamento deve mettere in atto misure tecniche e organizzative adeguate per assicurare un livello di sicurezza adeguato al rischio, previste dall'art. 32 GDPR, che comprendono, tra le altre, se del caso:

a) la pseudonimizzazione e la cifratura dei dati personali;
b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Tali misure devono assicurare un elevato livello di sicurezza. Nella valutazione del rischio per la sicurezza dei dati il Responsabile del trattamento deve tenere in considerazione i rischi presentati dal trattamento dei dati personali come la distruzione accidentale o illegale, la perdita, la modifica, la rivelazione o l'accesso non autorizzati a dati personali trasmessi, conservati o comunque elaborati, che potrebbero cagionare in particolare un danno fisico, materiale o immateriale. Il Responsabile del trattamento, se necessario e su richiesta, dovrà altresì assistere il Titolare del trattamento nella redazione del "DPIA" (Data Protection lmpact Assessment), contenente la valutazione sulla particolare probabilità e gravità del rischio inerente alle operazioni di trattamento da effettuare (tenuto conto della natura, dell'ambito di applicazione, del contesto, delle finalità e delle fonti di rischio) e sulle misure tecniche ed organizzative da adottare al fine di attenuare tale rischio assicurando la protezione dei dati personali e la conformità al GDPR. Se del caso, il Responsabile dovrà richiedere in merito un parere al DPO (Data Protection Officer) (art.35 e C.90 GDPR).

**Violazione dei dati**. Se dovesse venire a conoscenza di una violazione dei dati personali (Data Breach), il Responsabile, senza ingiustificato ritardo, deve informare per iscritto il Titolare del trattamento affinché possa procedere, se del caso, a notificare la violazione all'autorità di controllo competente (art.33 GDPR) e, qualora la violazione dei dati personali in questione dovesse essere suscettibile di presentare un elevato rischio per i diritti e le libertà delle persone fisiche, il Titolare del trattamento provvederà a darne comunicazione all'interessato (art.34 GDPR).

Il Responsabile deve coadiuvare il Titolare del trattamento nella redazione di specifiche procedure che consentono di individuare prontamente le violazioni dei dati subite (Data Breach) e le relative procedure di risposta attraverso l'elaborazione di una specifica policy.

La suddetta policy deve includere, tra le altre cose:

- le linee guida per valutare le violazioni di dati subite al fine di individuare quelle che sono suscettibili di presentare un elevato rischio per i diritti e le libertà delle persone fisiche e che dunque dovranno essere notificate all'Autorità di controllo competente;
- le linee guida sulla scelta delle informazioni che saranno rese disponibili all'interessato dal Titolare del trattamento attraverso la comunicazione della violazione, se dalla valutazione precedentemente effettuata, fosse risultata suscettibile di presentare rischi elevati per i diritti e le libertà dell'interessato.

Il Responsabile dovrà aiutare il Titolare del trattamento a documentare per iscritto qualsiasi violazione di dati subita, le circostanze ad essa relative, le conseguenze e i provvedimenti adottati per porvi rimedio.

Nello specifico dovranno essere documentati:

a) la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
b) il nome e i dati di contatto de DPO (se nominato) o di altro punto di contatto presso cui l'Autorità di controllo competente potrà ottenere maggiori informazioni;
c) la descrizione delle probabili conseguenze della violazione dei dati personali;
d) le descrizioni delle misure adottate o di cui si propone l'adozione da parte del Titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuare i possibili effetti negativi.

Tale documentazione dovrà essere resa disponibile all'Autorità di controllo competente attraverso la procedura di notifica della violazione dei dati (Data breach) prevista dall'art. 33 comma 3 del GDPR.