UNIONE EUROPEA
FONDI STRUTTURALI EUROPEI
PON 2014-2020
PER LA SCUOLA - COMPETENZE E AMBIENTI PER L'APPRENDIMENTO - FESR
Ministero dell'Istruzione, dell'Università e della Ricerca
Dipartimento per la Programmazione
Direzione Generale per interventi in materia di edilizia scolastica, per la gestione dei fondi strutturali per l'istruzione e per l'innovazione digitale
Ufficio IV
MIUR

**ISTITUTO COMPRENSIVO NOVENTA DI PIAVE**
Via Guaiane – 30020 NOVENTA DI PIAVE (Venezia)
Tel. 0421/307516 - Fax 0421/307814 - Cod. Min. VEIC817005 - Cod. fisc. 93000020276
Sito Web: www.icnoventadipiave.edu.it E-mail: veic817005@istruzione.it
P.E.C: veic817005@pec.istruzione.it

**IL CONSIGLIO DI ISTITUTO dell'IC NOVENTA di PIAVE**

**VISTA** la Legge 241/1990;
**VISTO** il D.P.R. 352/1992;
**VISTO** il D.Lgs. n. 196/2003;
**VISTA** la Legge 15/2005;
**VISTO** il D.P.R. 184/2006;
**VISTO** il Regolamento UE 2016/679 c.d. GDPR

**CON DELIBERA n. 141/v del 25 giugno 2019**

**ADOTTA**

Il seguente **REGOLAMENTO PER L'ADEGUAMENTO AL GDPR (REG. UE 2016/679) E PER L'IMPOSTAZIONE DI UN SISTEMA PER LA GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI**

.

# TITOLO 1

## NORME di CARATTERE GENERALE

### Art. 1 - Premessa

Il regolamento europeo Reg. 2016/679 ("GDPR" – General Data Protection Regulation), in quanto regolamento e non direttiva, è immediatamente esecutivo dal 24.05.2018; poiché in taluni passaggi (es. art 32 – sicurezza del trattamento) il GDPR prescrive il raggiungimento di obiettivi, con ampio margine discrezionale, tuttavia, sulle modalità concrete attraverso le quali gli obiettivi possono/potranno essere raggiunti, il presente regolamento stabilisce le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante cui, nell'ambito specifico dell'Istituto Comprensivo Noventa di Piave:

- verranno raggiunti e mantenuti nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR;
- verrà organizzato il SGSI – Sistema per la Gestione della Sicurezza delle Informazioni;
- si attesterà, in caso di controllo/ispezione da parte degli organismi preposti, che l'Istituto è in regola con le prescrizioni del succitato Regolamento UE 2016/679.

### Art. 2 - Obiettivo del presente Regolamento

Il presente regolamento permette di raggiungere i seguenti obiettivi:

- implementare il principio fondamentale di responsabilizzazione ("accountability") introdotto dal GDPR, in

base al quale il Titolare deve, non solo conformarsi alle prescrizioni del GDPR, ma anche essere in grado di dimostrare la conformità raggiunta;

- indicare metodologie e prassi operative, specifiche per l'adeguamento alle prescrizioni del GDPR, tenendo conto del contesto specifico dell'Istituto Comprensivo Noventa di Piave;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare la procedura per testare, verificare periodicamente e valutare regolarmente l'efficacia delle misure tecniche ed organizzative da mettere in atto per assicurare un adeguato livello di sicurezza e di protezione dei dati;
- impostare un SGSI – Sistema di Gestione della Sicurezza delle Informazioni, che permetta di dimostrare che l'Istituto è conforme ai requisiti di sicurezza previsti dall'art. 32 del GDPR ed agli standard di sicurezza riconosciuti a livello internazionale.

### Art. 3 - Liceità dei trattamenti

Per ciascun trattamento effettuato, deve essere verificata e documentata per iscritto la liceità del trattamento stesso; nel caso di un soggetto pubblico quale l'Istituto Comprensivo Noventa di Piave, la liceità del trattamento deve essere individuata nella base giuridica, che giustifica/richiede il trattamento specifico.
La base giuridica è costituita da:

- mandato istituzionale dell'Istituto Comprensivo Noventa di Piave
- norme di legge di rango primario.

In ogni caso, si dovrà, inoltre, sempre verificare che non sussistano norme di legge che vietino esplicitamente uno specifico trattamento.

### Art. 4 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs. 196/2003, l'informativa contenga le seguenti informazioni:

- i dati di contatto del Responsabile della protezione dei dati;
- la base giuridica del trattamento;
- il tempo di conservazione dei dati personali o, in subordine, i criteri utilizzati per determinare tale periodo;
- gli ulteriori diritti dell'interessato introdotti dal GDPR.

### Art. 5 - Consenso al trattamento dei dati

Il GDPR mantiene un principio chiave introdotto dall'art. 18 del D.Lgs. 196/2003, e cioè che i soggetti pubblici non devono richiedere il consenso dell'interessato. Pertanto, sia nei moduli cartacei che nei form web, non si dovrà chiedere il consenso dell'interessato (mentre invece sarà sempre necessario fornire l'informativa).
In via del tutto residuale, è consentito che l'Istituto Comprensivo Noventa di Piave possa chiedere il consenso dei genitori, laddove trattasi di servizi/attività opzionali, di implementazione dell'Offerta Formativa da effettuarsi in orario curricolare o extracurricolare, di cui i genitori o tutori degli alunni potrebbero decidere di non usufruire; in tali casi tuttavia, il consenso ha di fatto la valenza di documentare e tenere traccia del fatto che gli esercenti la potestà genitoriale/tutoriale hanno deciso di fruire del servizio/attività proposta. Tali casistiche residuali sono precisamente individuate e codificate, e si possono ricondurre alle seguenti fattispecie:

- decisione di avvalersi di attività curricolari/extracurricolari di implementazione dell'offerta formativa e di conseguenza aderire ad iniziative che possono prevedere collaborazioni/cooperazioni/parternariati con altri Enti/Associazioni/Organizzazioni/Ditte;
- decisione di partecipare a uscite scolastiche/viaggi di istruzione/iniziative progettuali particolari, e di conseguenza di aderire a forme di assicurazione
- decisione di avvalersi del servizio di trasporto scolastico, e di conseguenza di aderire a forme di assicurazione.

### Art. 6 – Ex incaricati del trattamento dei dati/Sub Responsabili – Unità Organizzative

Mentre il D.Lgs. 196/2003 prevedeva esplicitamente la figura dell'Incaricato del trattamento dei dati, il GDPR tratta la figura dell'incaricato in termini molto generali *all'Art. 29 – Trattamento sotto l'autorità del Titolare*

*del trattamento o del Responsabile del trattamento*, laddove specifica che "il Responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del Titolare del trattamento, che abbia accesso ai dati personali, non può trattare tali dati se non è istruito in tal senso dal Titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri.
Pertanto, ai sensi del suddetto Art. 29 all'interno dell'IC Noventa di Piave:

- sono state revocate le preesistenti nomine ad incaricato del trattamento dei dati;
- sono state individuate ed istituite 4 diverse UNITA' ORGANIZZATIVE, ovvero:
    1. Unità Organizzativa 1: Ufficio di Segreteria
    2. Unità organizzativa 2: Collaboratori scolastici
    3. Unità Organizzativa 3: Docenti
    4. Unità organizzativa 4: Esperti Esterni
- sono stati individuati, all'interno di ciascuna UNITA' ORGANIZZATIVA di cui al punto precedente, i SUB-RESPONSABILI designati quali incaricati del trattamento dati;
- sono stati designati -con specifico decreto di nomina- ed istruiti con Atto Formale tutti i SUB-RESPONSABILI di ciascuna UNITA' ORGANIZZATIVA.

## Art. 7 - Non applicabilità del requisito della portabilità dei dati

L'art. 20 del GDPR prevede astrattamente, in relazione ai trattamenti automatizzati, il diritto da parte dell'interessato (i cui dati sono stati conferiti con il suo consenso esplicito o su base contrattuale) alla portabilità dei dati. Tuttavia l'Istituto Comprensivo Noventa di Piave non è tenuto a soddisfare le richieste di portabilità dei dati, in quanto:

- non si applica si applica la portabilità ai dati che vengono trattati sulla base dell'interesse pubblico o nell'adempimento di obblighi di legge del titolare o per scopi di archiviazione nel pubblico interesse.

## Art. 8 - Tempi di conservazione dei dati e regole di scarto

Per quanto le modalità, in ottemperanza all'art. 5 del GDPR, tutti i dati saranno conservati -nelle forme che consentono l'identificazione degli interessati- per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali potranno essere conservati per periodi più lunghi se trattati esclusivamente ai fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici. Per quanto attiene i tempi di conservazione dei dati contenuti in documenti amministrativi e le relative regole di scarto, si applicano le prescrizioni emesse dalla articolazione regionale di riferimento della Soprintendenza Archivistica e/o quelle recepite a livello di Regolamento di Protocollo e di Manuale per la Gestione dei Flussi Documentali.

## Art. 9 – Referenti/Responsabili del trattamento

All'interno dell'Istituto Comprensivo Noventa di Piave, viene data facoltà di designare in qualità di Referenti Interni del trattamento dei dati i titolari di articolazione organizzativa apicale, con particolare riferimento alla figura del DSGA (Direttore dei Servizi Generali ed Amministrativi) e dei Referenti dei Plessi in cui si articola l'IC Noventa di Piave.
A seconda della tipologia di dati trattati e dei trattamenti effettuati, è possibile designare in qualità di Responsabile esterno del trattamento dei dati, i soggetti esterni all'Istituto Comprensivo Noventa di Piave coinvolti a vario titolo nelle varie operazioni di trattamento dei dati, come ad esempio le ditte incaricate dei servizi di assistenza e manutenzione dei degli apparati hardware oppure delle piattaforme software, con particolare riferimento alle piattaforme in cloud (es. registro elettronico, segreteria digitale, gestionale in cloud per il personale, etc.). Nello specifico sono stati designati Responsabili Esterni -attraverso "Contratto di nomina a responsabile del trattamento dei dati personali ai sensi dell'articolo 28, Regolamento (UE) 2016/679" appositamente stipulato- i Titolari delle seguenti Ditte/Aziende:

1. Spazio Sputnik Srls, con sede legale in Via Armstrong 1, 30020 Quarto d'Altino (VE), nella persona del titolare, Sig. Mirko Visentin (ditta incaricata della gestione/manutenzione del sito istituzionale dell'IC Noventa di Piave)
2. Argo Software s.r.l., 97100 RAGUSA, nella persona del legale rappresentante, prof. Lorenzo Lo Presti (ditta titolare della piattaforma software per la gestione digitale del personale della scuola);

3. D & C – DESIGN AND CONSULTING s.r.l., nella persona dell'Amministratore Unico, Sig. Lorenzo Bortolato (ditta incaricata dei servizi di assistenza e manutenzione dei degli apparati hardware);
4. Gruppo Spaggiari PARMA S.p.A., nella persona del presidente, Dott. Pier Paolo Avanzi (ditta titolare della piattaforma software per la gestione digitale della Segreteria, del Registro Elettronico, degli alunni).

# TITOLO 2

## SICUREZZA

### Art. 10 - Premessa

Al fine di garantire un'adeguata sicurezza dei dati trattati, saranno messe in atto apposite misure di protezione, attraverso l'approntamento di soluzioni tecniche (autenticazione, autorizzazione, cifratura dei dati, separazione , firewall, antivirus, business continuity, disaster recovery, intrusion detection, vulnerability assessment/penetration teste) e organizzative (nomina per iscritto personale, istruzioni per il trattamento, accesso controllato, armadi chiusi, procedura modifica credenziali, policy aziendale, formazione, nomina per iscritto responsabili esterni) idonee ad evitare trattamenti non autorizzati o illeciti, perdite, distruzioni o danni accidentali.

### Art. 11 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati

Nel caso si verifichi un qualsiasi tipo di violazione dei dati, o se ne abbia anche solamente il sospetto, ne deve essere data immediata comunicazione al Dirigente Scolastico e al Responsabile della protezione dei dati, il quale si attiverà immediatamente per valutare:

- se vi sia stata effettivamente una violazione, la portata e le conseguenze,
- se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

### Art. 12 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5 del GDPR, deve essere in ogni caso tenuto un registro di tutte le violazioni di dati verificatesi, a prescindere dal fatto che siano state notificate all'autorità di controllo. Il suddetto registro deve contenere come minimo le seguenti informazioni:

- data della violazione
- descrizione delle circostanze e dell'evento
- tipologia e quantità di interessati impattati
- conseguenze della violazione
- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

In data 24 maggio 2018, con prot. n. 5175/2018, è stato istituito con decreto del DS il *Registro delle Violazioni dati personali (Data Breach)* dell'IC Noventa di Piave.

### Art. 13 - Il modello MMS – Modello per il Monitoraggio della Sicurezza

La sicurezza può continuamente essere compromessa da una serie di eventi che possono accadere. Questi eventi devono pertanto essere tracciati ed essere oggetto di analisi periodica.
La tracciatura degli eventi si effettua compilando il Modello MMS – Modello per il Monitoraggio della Sicurezza, con frequenza trimestrale; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR.

**Art. 14 - Il modello DMS – Documento sul Monitoraggio della Sicurezza**

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno semestrale, all'interno di un documento denominato DMS – Documento per il Monitoraggio della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto all'attenzione del Dirigente Scolastico. All'interno del DMS devono inoltre trovare trattazione esaustiva ed organica tutte le problematiche relative alla sicurezza e alla protezione dei dati personali che si sono verificate nel semestre di riferimento, come ad esempio:

- l'esternalizzazione di un nuovo trattamento di dati
- la predisposizione di una procedura operativa o di un regolamento ad- hoc
- la predisposizione di una lettera di nomina
- la predisposizione di una nuova informativa
- la predisposizione di comunicazioni ai dipendenti o agli interessati
- il recepimento di norme o linee guida emesse a livello nazionale od europeo, concernenti la sicurezza o la protezione dei dati
- l'analisi di una richiesta di accesso ai dati
- la revisione dei Registri del trattamenti dei dati
- lo svolgimento di un DPIA – Data Protection Impact Assessment
- la verifica del soddisfacimento dei principi di Privacy by Design e Privacy by default all'interno di un sistema o di un processo.

**Art. 15 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati**

Poiché l'art. 32 del GDPR lascia un ampio margine di discrezione sulle prassi da mettere in atto per assicurare un adeguato livello di sicurezza, in fase di prima applicazione del GDPR e per un periodo transitorio di 24 mesi a far data dal 25 maggio 2018, dovranno comunque essere messe in atto le misure minime di sicurezza previste dagli artt. 33, 34 e 35 del D.Lgs. 196/2003, nei modi previsti dal Disciplinare Tecnico (Allegato B al D.Lgs. 196/2003), nonché le misure minime di sicurezza per tutte le PA previste dalla Circolare AGID 2/2017.
Parimenti, in fase di prima applicazione del GDPR e per un periodo di 24 mesi a far data dal 25 maggio 2018, si dovranno seguire le prescrizioni dell'atto di natura regolamentare adottato dall'Ente ai sensi degli artt. 20 e 21 del D.Lgs. 196/2003.

**Art. 16 - Il Comitato SP – Comitato per la Sicurezza e la Privacy**

Per assicurare un adeguato livello di attenzione e di potere decisionale in merito a tutte le questioni riguardanti la sicurezza e la protezione dei dati personali, deve essere costituito un Comitato per la Sicurezza e la Privacy (per brevità denominato "Comitato SP"), costituito dai seguenti membri permanenti:

- Il Titolare del trattamento dati, Dirigente Scolastico
- Il Referente interno del trattamento dati, D.S.G.A.
- Responsabile della protezione dei dati.

Il suddetto Comitato si deve riunire con frequenza almeno semestrale, per analizzare tutte le problematiche inerenti la sicurezza e la privacy che si sono verificate nel periodo di riferimento e analizzare tutti i modelli MMS e DMS prodotti. Alla fine di ogni riunione del Comitato deve essere prodotto un verbale delle principale decisioni prese.

**Art. 17 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR**

In caso di verifiche da parte del Garante per la protezione dei dati o della Guardia di Finanza o delle autorità preposte, l'Istituto Comprensivo Noventa di Piave deve poter dimostrare di aver messo in atto un sistema di gestione della sicurezza tale da soddisfare i requisiti previsti dall'art. 32 del GDPR.
A tal fine è di fondamentale importanza quanto enunciato dall'art. 32 comma 3 del GDPR, laddove si specifica che l'adesione a codici di condotta approvati o ad uno scherma di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

**Art. 18 - Verifiche e certificazioni periodiche da parte del Responsabile della protezione dei dati**

In ottemperanza a quanto previsto dagli artt. 37, 38 e 39 del GDPR, il Responsabile della protezione dei dati è tenuto ad effettuare, con frequenza almeno quadrimestrale, verifiche finalizzate ad accertare che i

trattamenti e le prassi messe in atto dall'Istituto Comprensivo Noventa di Piave sono conformi a quanto prescritto dal GDPR; oppure, in caso di non conformità, il Responsabile della protezione dei dati è tenuto a documentare le non conformità riscontrate e ad individuare e descrivere le misure correttive da mettere in atto, specificando inoltre il termine entro il quale le suddette misure devono essere messe in atto e i soggetti coinvolti.

**Art. 19 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione**

Coerentemente con quanto previsto dall'art. 32 comma 3 del GDPR, l'Istituto Comprensivo Noventa di Piave ha facoltà di ricorrere a codici di condotta e a schemi di certificazione per dimostrare la conformità ai requisiti di cui all'art. 32 comma 1 del GDPR.

Allorquando i suddetti codici di condotta e/o schemi di certificazione siano stati emessi dal Garante per la protezione dei dati personali ed approvati rispettivamente ai sensi degli artt. 40 e 42 del GDPR, viene data facoltà all'Istituto Comprensivo Noventa di Piave di aderire ai suddetti codici e schemi, con il coordinamento e la consulenza del Responsabile della protezione dei dati.