



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dmilani@libero.it- vaic83400c@istruzione.it
sib web : www.comprensivovergiate.edu.it



Indice

SEZIONE 1 – PARTE GENERALE.....	3
Art. 1 - Premessa.....	3
Art. 2 - Obiettivo del presente Regolamento	4
Art. 3 - Liceità dei trattamenti	5
Art. 4 - Informativa agli interessati.....	6
Art. 5 - Consenso al trattamento dei dati	6
Art. 6 - Incaricati del trattamento dei dati.....	7
Art. 7 - Non applicabilità del requisito della portabilità dei dati	8
Art. 8 - Tempi di conservazione dei dati e regole di scarto	9
Art. 9 - Responsabili del trattamento	9
SEZIONE 2 – SICUREZZA	10
Art. 10 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati.....	10
Art. 11 - Registro delle violazioni dei dati.....	11
Art. 12 - Il modello MMS – Modello per il Monitoraggio della Sicurezza.....	12
Art. 13 - Il modello DMS – Documento sul Monitoraggio della Sicurezza.....	14
Art. 14 - Requisiti per il raggiungimento di un adeguato livello di sicurezza nei trattamenti effettuati.....	15
Art. 15 - Il Comitato SP – Comitato per la Sicurezza e la Privacy.....	16
Art. 16 - Dimostrazione della conformità ai requisiti di sicurezza previsti dall'art. 32 del GDPR.....	17
Art. 17 - Verifiche e certificazioni periodiche da parte del Responsabile della protezione dei dati.....	Errore. Il segnalibro non è definito.
Art. 18 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione.....	18



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297 – Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dimilani@libero.it- vaic83400c@istruzione.it
sito web : www.comprensivovergiate.edu.it



SEZIONE 1 – PARTE GENERALE

Art. 1 - Premessa

Il regolamento europeo Reg. 2016/679 (“GDPR” – General Data Protection regulation), in quanto regolamento e non direttiva, è immediatamente esecutivo e pertanto non necessita di alcun recepimento o approvazione.

Il presente regolamento pertanto non concerne il recepimento del GDPR, cosa che non avrebbe alcun senso ne’ da un punto di vista concettuale, ne’ dal punto di vista pratico.

Tuttavia, il GDPR in alcuni punti (es. art 32 – sicurezza del trattamento) enuncia delle affermazioni di principio o degli obiettivi da raggiungere, lasciando ampio margine discrezionale sulle modalità concrete attraverso le quali gli obiettivi possono venire raggiunti.

Modalità che dipendono da molteplici fattori, tra i quali le dimensioni, l’organizzazione, la cultura, le competenze e le dotazioni dell’Ente.

Il presente documento serve pertanto a individuare con precisione le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali, nell’ambito specifico dell’Istituto, si raggiunge e si mantiene nel tempo l’adeguamento e la



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dilmilani@libero.it- vaic83400c@istruzione.it
web : www.comprensivovergiate.edu.it



conformità alle prescrizioni del GDPR e si imposta un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni e si possa dimostrare, in caso di controlli o ispezioni 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 essere conforme alle prescrizioni del GDPR, ma deve 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’Ente;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una procedura per testare, verificare periodicamente e



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fisc. 82014720120 Codice Univoco UFIFMP

e-mail: dimilani@libero.it- vaic83400c@istruzione.it

web : www.comprensivovergiate.edu.it



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 e conforme a riconosciuti standard di sicurezza 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 come l'Istituto, la liceità del trattamento deve essere individuata nella base giuridica che giustifica/richiede il trattamento specifico.

La base giuridica deve essere può essere costituita da:

- funzioni istituzionali dell'Ente, oppure
- norme di legge di rango primario.

Si dovrà inoltre verificare che non sussistano norme di legge che vietino esplicitamente il trattamento.



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dilmilani@libero.it- vaic83400c@istruzione.it
web : www.comprensivovergiate.edu.it



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, se non è possibile, 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 è necessario fornire l'informativa).



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dlmilani@libero.it- vaic83400c@istruzione.it
sib web : www.comprensivovergiate.edu.it



In via del tutto residuale, è consentito che l'Istituto possa chiedere il consenso dei genitori, laddove trattasi di servizi opzionali, 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 la famiglia/il tutore ha deciso di usufruire del servizio. Tali casistiche residuali sono precisamente individuate e codificate, e si possono ricondurre alle tre seguenti fattispecie:

- decisione di avvalersi del servizio di ristorazione scolastica
- decisione di partecipare a gite scolastiche, 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 - Incaricati del trattamento dei dati

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 più 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



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail dimilani@libero.it- vaic83400c@istruzione.it
s it web : www.comprensivovergiate.edu.it



dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri. Nel caso dell'Istituto, per chiarezza si continuerà ad usare la dicitura "Incaricato del trattamento dei dati", intendendo con tale locuzione i soggetti di cui all'art. 29 del GDPR. Ai fini del GDPR, continuano ad essere valide le preesistenti nomine ad incaricato del trattamento dei dati, che si intendono rinnovate ai sensi dell'art. 29 del GDPR. E' data comunque facoltà di integrare o modificare o revocare esplicitamente le preesistenti nomine ad incaricato del trattamento dei dati, oppure di emettere nuovi atti di nomina secondo i quali le persone fisiche vengono denominati soggetti "designati" ai sensi del GDPR.

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

L'art. 20 del GDPR prevede astrattamente il diritto dalla parte dell'interessato alla portabilità dei dati. Tuttavia l'Istituto non è tenuto a soddisfare le richieste di portabilità dei dati, in quanto:

- la portabilità dei dati non si applica ai dati in formato cartaceo
- la portabilità dei dati non si applica ai trattamenti che prescindono dal consenso.



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail dlmilani@libero.it- vaic83400c@istruzione.it
sit web : www.comprensivovergiate.edu.it



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

Per quanto riguarda i tempi di conservazione dei dati 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 - Responsabili del trattamento

Il GDPR ha introdotto una significativa novità a livello organizzativo, consistente nel fatto che i tradizionali responsabili “interni” del trattamento dei dati non possono più essere designati.

L’art. 28 del GDPR prevede una figura di “responsabile del trattamento” che può essere ricoperta solo da soggetti esterni.



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail dlmilani@libero.it- vaic83400c@istruzione.it
sit web : www.comprensivovergiate.edu.it



Alla luce di quanto detto sopra, a seconda della tipologia di dati trattati e dei trattamenti effettuati, è possibile designare in qualità di Responsabile esterno del trattamento dei dati il soggetto esterno all'Ente coinvolto a vario titolo nelle varie operazioni di trattamento dei dati, come ad esempio 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, protocollo informatico in cloud, etc.).

SEZIONE 2 – SICUREZZA

Art. 10 - Obbligo di notificazione immediata di una violazione dei dati al Responsabile della protezione dei dati



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297 – Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP

e-mail: dlmilani@libero.it- vaic83400c@istruzione.it

siò web : www.comprensivovergiate.edu.it



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, e valutare se sussistano i presupposti per effettuare la notificazione entro 72 ore all'autorità di controllo.

Art. 11 - Registro delle violazioni dei dati

Coerentemente con quanto previsto dall'art. 33 comma 5, 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



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C
Cod. Fis. 82014720120 Codice Univoco UFIFMP
e-mail: dilmilani@libero.it- vaic83400c@istruzione.it
s b web : www.comprensivovergiate.edu.it



- data di comunicazione della violazione al Garante per la protezione dei dati (se la comunicazione è stata effettuata).

Art. 12 - 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 settimanale o mensile; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR, alla mail

mms@capitalsecurity.it



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fic. 82014720120 Codice Univoco UFIFMP

e-mail: dilmilani@libero.it- vaic83400c@istruzione.it

sito web : www.comprensivovergiate.edu.it



Art. 13 - Effettuazione periodica di scansioni di vulnerabilità sulle piattaforme in cloud

Coerentemente con le linee guida strategiche ed operative contenute nel Piano di Informatizzazione della Pubblica Amministrazione, la Pubblica Amministrazione utilizza sempre più frequentemente ed in modo significativo le piattaforme in cloud, che hanno il vantaggio tra l'altro di permettere una significativa riduzione dei costi di possesso (TCO – Total Cost of Ownership) e di gestione.

Una delle piattaforme in cloud più importanti utilizzate in ambito scolastico è il Registro Elettronico, che appunto essendo in cloud è esposto a tutta una serie di attacchi. Per questo è importante che vengano effettuate periodicamente delle scansioni di vulnerabilità per individuare e documentare debolezze e configurazioni poco sicure, e per svolgere le attività di remediation.

Le scansioni di vulnerabilità verranno effettuate a cura del Responsabile della protezione dei dati con frequenza orientativamente bimestrale (ogni due mesi) utilizzando la piattaforma professionale a pagamento Qualys, leader nei servizi di vulnerability assessment.

Come minimo le scansioni dovranno essere effettuate sulle due seguenti piattaforme:

- Registro Elettronico



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari, 2

Tel. 031 946 297 – Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP

e-mail: dlmilani@libero.it - vaic83400c@istruzione.it

site web : www.comprensivovergiate.edu.it



- Sito web istituzionale.

A fronte di richiesta da parte del Dirigente Scolastico o del DSGA, delle scansioni una-tantum potranno venire effettuate su altri oggetti esposti direttamente su internet, come ad esempio firewall, router, server di posta elettronica etc.

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

Gli eventi di cui all'articolo 12 devono essere oggetto di analisi periodica all'interno di un documento denominato MMS – Documento per il Monitoraggio della Sicurezza, predisposto dal Responsabile della protezione dei dati e posto all'attenzione del Dirigente Scolastico e del Comitato per la Sicurezza e la Privacy. 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 trimestre 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



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale

21029 Vergiate (VA) – Largo Lazzari , 2

Tel. ☎ 031 946 297 – Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP

e-mail: dlmilani@libero.it- vaic83400c@istruzione.it

si web : www.comprensivovergiate.edu.it



- 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 dei 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



Ministero dell'Istruzione, dell'Università e Ricerca
Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C
Cod. Fisc. 82014720120 Codice Univoco UFIFMP
e-mail : dlmilani@libero.it- vaic83400c@istruzione.it
sito web : www.comprensivovergiate.edu.it



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:

- Dirigente Scolastico
- D.S.G.A. o soggetto equivalente per gli Istituti parificati



Ministero dell'Istruzione, dell'Università e Ricerca

Istituto Comprensivo Statale
21029 Vergiate (VA) – Largo Lazzari , 2

Tel. 031 946 297– Fax 0331 964 006 - Cod. Scuola
VAIC83400C

Cod. Fis. 82014720120 Codice Univoco UFIFMP

e-mail: dimilani@libero.it- vaic83400c@istruzione.it

web : www.comprensivovergiate.edu.it



Sicurezza delle Informazioni conforme (ad esempio) ai seguenti standard
internazionali di sicurezza:

- ISO / IEC 27001 (norma vera e propria)
- ISO / IEC 27002 (best practice e raccomandazioni in materia di sicurezza)
- Annex-A ("Control Objectives and Controls").