# Modello Organizzativo e Disposizioni Operative per l'adeguamento al GDPR (Reg. UE 2016/679)

| | |
|---|---|
| **Nome documento**: | Modello Organizzativo e Disposizioni Operative per l'adeguamento al Regolamento UE 2016/679 (GDPR) |
| **Codice documento**: | 3.Registro Adeguamento GDPR Ver 1.2 |
| **Nome file**: | 3.Registro Adeguamento GDPR Ver 1.2 |
| **Stato documento**: | Definitivo |
| **Versione**: | 1.2 |
| **Data creazione**: | 28 maggio 2018 |
| **Data ultimo aggiornamento** | 10 gennaio 2019 |

# Indice

# SEZIONE 1 – PARTE GENERALE

## Art. 1 - Premessa

Il presente documento si prefigge di individuare le modalità, le prassi, la metodologia, le tecniche e gli strumenti mediante le quali si intende raggiungere e mantenere nel tempo l'adeguamento e la conformità alle prescrizioni del GDPR; inoltre esso permette di impostare un SGSI – Sistema per la Gestione della Sicurezza delle Informazioni e permette di 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'Istituto;
- in particolare, per quanto riguarda la sicurezza (art. 32), individuare precisamente una 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 e conforme a riconosciuti standard di sicurezza a livello internazionale.

## Art. 3 - Ammissibilità 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'Istituto, oppure
- norme di legge di rango primario.

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

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 come da seguente elenco:

- decidere di avvalersi del servizio di ristorazione scolastica;
- decidere di partecipare ad attività facoltative (visite d'istruzione, rappresentazioni teatrali, incontri, stage, ecc.);
- aderire a forme di assicurazione;
- decidere di avvalersi del servizio di trasporto scolastico;
- aderire a forme di assicurazione;
- comparire in riprese videofotografiche;

## Art. 6 - Incaricati del trattamento dei dati (designati)

Nel caso dell'Istituto, per semplicità si userà 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 da parte dell'interessato alla portabilità dei dati. Tuttavia l'Istituto può non 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;
- la portabilità dei dati è vincolata alle norme previste da funzioni istituzionali dell'Istituto, oppure da norme di legge di rango primario.

## 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

Si procederà alla designazione di Responsabile del trattamento dei dati il soggetto esterno all'Istituto coinvolto a vario titolo nelle varie operazioni di trattamento dei dati, come:

professionisti od aziende incaricate dei servizi di assistenza e manutenzione dei degli apparati hardware e/o delle piattaforme software,

aziende titolari delle 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

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 all'autorità di controllo entro 72 ore dall'evento.

## Art. 11 - Registro delle violazioni dei dati e di monitoraggio della sicurezza (Registro monitoraggio sicurezza)

Coerentemente con quanto previsto dall'art. 33 comma 5, è stato predisposto un registro per l'annotazione di tutti gli eventi significativi verificatisi anche se non notificati all'autorità di controllo.

Gli eventi che necessitano della segnalazione all'autorità garante saranno approfonditi in una specifica sezione di detto registro

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 Registro per il Monitoraggio della Sicurezza, con frequenza settimanale; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR.

Gli eventi di cui al paragrafo precedente devono essere analizzati con frequenza almeno trimestrale, all'interno di un documento denominato Registro 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 RMS 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
- 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.12 - 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'Istituto ai sensi degli artt. 20 e 21 del D.Lgs. 196/2003.

## Art.13 - 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.
- Responsabile della protezione dei dati.

Il suddetto Comitato si deve riunire con frequenza almeno semestrale (ogni sei mesi), 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. ?? (per esempio quello di qualche giorno fa)

## Art.14 - 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 deve essere in grado di dimostrare che ha 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 schema di certificazione (come l'insieme della presente documentazione) può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

## Art.15 - 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 a verificare e certificare il fatto che i trattamenti e le prassi messe in atto dall'Istituto 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.