Istituto Comprensivo Iqbal Masih

Modello Organizzativo e Disposizioni Operative per l'adeguamento al GDPR (Reg. UE 2016/679) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni secondo gli standard internazionali ISO 27001 e 27002

Nome documento:	Modello Organizzativo e Disposizioni Operative per l'adeguamento al Regolamento UE 2016/679 (GDPR) e per l'impostazione di un Sistema per la Gestione della Sicurezza delle Informazioni
Codice documento:	IC e IS – Reg Adeguamento GDPR Ver 1-0.doc
Nome file:	IC e IS – Reg Adeguamento GDPR Ver 1-0.doc
Stato documento:	Definitivo
Versione:	1.1
Data creazione:	26 luglio 2018
Data ultimo aggiornamento	31 agosto – Prot.n.1608/A39

NB: Il presente Documento viene depositato agli atti in forma cartacea il 31 agosto di ogni anno nella versione definitiva di inizio anno scolastico, mentre la sua versione digitale viene aggiornata e pubblicizzata quando necessario (a disposizione degli interessati), per essere stampata e sostituire quella precedente al 31 agosto dell'anno successivo.

Indice

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 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.

Vanno quindi in premessa sinteticamente evidenziati sia i SOGGETTI coinvolti in diverse forme di trattamento, sia gli OGGETTI del trattamento (intesi come sistemi diversi di creazione/conservazione/scambio dei dati degni di tutela).

SOGGETTI:

Al di là dei Responsabili esterni (elencati in allegato al Registro delle attività di trattamento), nell'Istituto assumono il ruolo di incaricato/designato al trattamento di dati tutte le unità di personale con alcune distinzioni:

- il personale di Segreteria per il trattamento dei dati digitali e materiali relativi a personale, utenza e terzi;
- i Docenti per il trattamento di alcuni dati digitali e materiali relativi a utenza e personale;
- i Collaboratori Scolastici per il trattamento di alcuni dati materiali relativi a utenza e personale;
- vanno poi ricordati i Genitori eletti quali Rappresentanti che trattano dati digitali e materiali relativi all'utenza – p.es. recapiti relativi ad altri Genitori;

In tutti i casi la designazione avviene da parte del DS, lo scambio di credenziali/ autorizzazioni avviene tramite intervento del DSGA e l'assunzione individuale delle corrispondenti responsabilità di riservatezza e di custodia dei dati ha luogo con sottoscrizione valida per tutto il periodo di permanenza nell'Istituto;

OGGETTI:

I diversi sistemi di creazione/conservazione/scambio dei dati in uso nell'Istituto possono essere distinti tra cartacei e digitali ed entrambi vanno a loro volta suddivisi tra sfera didattica (alunni e famiglie per gli aspetti educativi, didattici e di reperibilità) e sfera amministrativa (personale ed interlocutori esterni, oltre ad alunni e famiglie per gli aspetti burocratici).

Il sistema carataceo nella sfera amministrativa trova i propri archivi sotto la responsabilità della Segreteria in locali ed armadi specifici, con chiusura a chiave negli orari di mancato utilizzo, con sistema antintrusione.

Il sistema cartaceo nella sfera didattica trova i propri archivi sotto la responsabilità dei docenti, del dirigente e (per alcuni aspetti) dei Collaboratori Scolastici, gli archivi presenti nei locali scolastici prevedono la chiusura a chiave negli orari di mancato utilizzo, con sistema antintrusione.; la documentazione didattico-educativa che i docenti detengono in archivi personali ricade interamente sotto la loro personale responsabilità di custodia e riservatezza.

Vi è poi il sistema cartaceo della corrispondenza riservata, detenuto nei locali della direzione sotto la diretta responsabilità del dirigente scolastico; in tal caso si ha

il trattamento di dati generalmente sensibili, che per tale motivo è stato sottratto ai sistemi digitali, scegliendo invece un archivio esclusivamente cartaceo che prevede la chiusura a chiave negli orari di mancato utilizzo, con sistema antintrusione.

Il sistema digitale nella sfera amministrativa si avvale di una rete dedicata, ad accesso selezionato, con adeguati sistemi di salvataggio, amministrata dal docente incaricato e dalla Ditta di servizio tecnico (vedi Allegato al Registro dei trattamenti). Vengono utilizzati diversi sistemi gestionali esterni – Axios, SIDI, Nuvola - (vedi Allegato al Registro dei trattamenti), frutto di liberi contratti o di scelte ministeriali, anch'essi ad accesso selezionato e con adeguati sistemi di salvataggio.

Il sistema digitale nella sfera didattica si avvale in ogni sede di una rete dedicata, ad accesso selezionato, con adeguati sistemi di salvataggio, amministrata dal docente incaricato e dalla Ditta di servizio tecnico (vedi Allegato al Registro dei trattamenti). In questo campo viene utilizzato un solo sistema gestionale esterno – Registro elettronico Nuvola - (vedi Allegato al Registro dei trattamenti), frutto di libero contratto, inibito agli utenti, anch'esso ad accesso selezionato e con adeguati sistemi di salvataggio.

La documentazione didattico-educativa in formato elettronico che i docenti detengono in dispositivi personali ricade interamente sotto la loro personale responsabilità di custodia e riservatezza.

La documentazione di carattere generale pubblicata sul Sito di Istituto sotto la responsabilità del dirigente scolastico contiene dati relativi al Personale ed all'Utenza nei limiti dell'indispensabilità legata alle responsabilità professionali da rendere pubbliche; la parte riservata del Sito (accessibile esclusivamente al Personale con gli stessi vincoli e modalità sopra citati) pone ai soggetti autorizzati le stesse responsabilità di riservatezza validi per tutta la documentazione professionale a cui hanno accesso.

Art. 2 - Obiettivo del Regolamento UE

Il nuovo regolamento europeo 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 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 è 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.

Art. 4 - Informativa agli interessati

Il GDPR prevede che, oltre a quanto già previsto dall'art. 13 del D.Lgs. 196/2003, le informative utilizzate contengano 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. 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.

L'Istituto può inoltre richiedere il consenso per altri trattamenti derivanti da esigenze organizzative e per altre situazioni contingenti.

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 e responsabilizzato in tal senso 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. Essi vengono in ogni caso individuati annualmente con la emissione di specifica Circolare contemporanea al rinnovo annuale del presente documento.

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

L'art. 20 del GDPR prevede astrattamente il diritto dal 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.

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 generalmente non possono più essere designati.

L'art. 28 del GDPR prevede una figura di "responsabile del trattamento" che può essere ricoperta generalmente da soggetti esterni.

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

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
- 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 mensile ~~settimanale~~; il modello compilato deve essere inviato al Responsabile della protezione dei dati designato ai sensi dell'art. 37 del GDPR alle scadenze convenute.

Art. 13 - Il modello DMS – Documento sul Monitoraggio della Sicurezza

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno semestrale ~~trimestrale~~, 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 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 semestre ~~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. 14 - 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. 15 - 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
- Responsabili interni di eventuali Servizi Digitali
- 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.

Art. 16 - 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 scherma di certificazione può essere addotto come elemento per comprovare la conformità ed un adeguato livello di sicurezza e di protezione dei dati.

Art. 17 - 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.

Art. 18 - Gestione della sicurezza secondo codici di comportamento o meccanismi di certificazione

Coerentemente con quanto previsto dall'art. 32 comma 3 del GDPR, l'Istituto 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 di

aderire ai suddetti codici e schemi, con il coordinamento e la consulenza del Responsabile della protezione dei dati.

Nel caso in cui i suddetti codici di condotta e/o meccanismi di certificazione approvati non siano stati ancora emessi dall'Autorità Garante per la protezione dei dati personali, viene data facoltà al Responsabile della protezione dei dati di valutare, proporre e coordinare l'eventuale adesione a schemi internazionali di certificazione di sicurezza, al fine di poter dimostrare la conformità ai requisiti dell'art. 32 del GDPR – Sicurezza del trattamento, secondo il principio di responsabilizzazione ("accountability"), e di mettere in atto un SGSI – Sistema per la Gestione della 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").