DELIBERA N° 06/2019

Il Consiglio d'Istituto nella seduta del 26/02/2019 alla quale erano presenti :

sig. COSTANZO Nevio- Presidente
Prof.ssa RIZZATTO Rossella– Dirigente scolastico reggente
prof. GONANO Luciano - Segretario

Componente docenti:
prof. BRESSAN Michele
prof.ssa INTINI Adele
prof.ssa CERA Gianna
prof.ssa MICCOLI Agnese
prof.ssa SPAZZINI Liliana
prof. BROTTO Alessandro
prof. PUZZI Alessandro

Componente genitori:

Componente Allievi:
UCCELLO Federico

Componente personale A.T.A:

non eletta

ed assenti:
Componente docenti:

Componente Allievi:
PARISE Luca
DE LILLO Giorgio

Componente genitori:

ha assunto la seguente deliberazione:

OGGETTO: Regolamento GDPR

IL CONSIGLIO D'ISTITUTO

VISTO la Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995
VISTO quanto già previsto dalla legge 675/1996 in attuazione alla Direttiva 95/46/CE del Parlamento Europeo
VISTO quanto già previsto dall'art. 13 del D.Lgs. 196/2003;
VISTO quanto già previsto dall'art. 18 del D.Lgs. 196/2003;
VISTO che 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;

D E L I B E R A (delibera n. 06/2019)

di approvare i seguenti regolamenti:
a) 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

ISTITUTO STATALE D'ISTRUZIONE SUPERIORE "G. GALILEI"
Settore Tecnologico "G.Galilei" - "N. Pacassi" – Settore Economico "E. Fermi"
Sede legale: via Puccini, 22 - 34170 – GORIZIA - tel. 0481.531452-530048 - fax 0481.534955
Mail istituzionale: gois008001@istruzione.it - PEC: gois008001@pec.istruzione.it www.isitgo.it

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
Nome file:	DS_GDPR Scuole - DOC003 - Reg Adeguamento GDPR V 2.0
Stato documento:	Definitivo

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.

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 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.

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. 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 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 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 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.

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

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

Gli eventi di cui all'articolo precedente devono essere analizzati con frequenza almeno 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 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 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. 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
- 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 a cura del DPO un verbale delle principali 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 entro il 31-7-2018 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'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").

b) Disposizioni operative per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione

ISTITUTO STATALE D'ISTRUZIONE SUPERIORE "G. GALILEI"
Settore Tecnologico "G.Galilei" - "N. Pacassi" – Settore Economico "E. Fermi"
Sede legale: via Puccini, 22 - 34170 – GORIZIA - tel. 0481.531452-530048 fax 0481.534955
E-MAIL: gois008001@istruzione.it - PEC: gois008001@pec.istruzione.it SITO WEB: www.isitgo.it

Titolo documento:	**Disposizioni operative per il riutilizzo e lo smaltimento di apparecchiature elettroniche e supporti di memorizzazione**
Nome file:	DS_GDPR Scuole - DOC004 - REG RiutilizzoSmaltimento PC Ver 1.0
Stato documento:	Definitivo
Versione:	1.0

Indice

Art.1 - Definizioni

Di seguito si riportano alcune definizioni rilevanti ai fini del presente regolamento; per le altre definizioni si rimanda all'art. 4 del Regolamento UE 2016/679 – GDPR.

Ai fini del presente regolamento s'intende per:

1) **«dato personale»**: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale;

2) **«trattamento»**: qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione;

3) **«limitazione di trattamento»**: il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro;

4) **«profilazione»**: qualsiasi forma di trattamento automatizzato di dati personali consistente nell'utilizzo di tali dati personali per valutare determinati aspetti personali relativi a una persona fisica, in particolare per analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze personali, gli interessi, l'affidabilità, il comportamento, l'ubicazione o gli spostamenti di detta persona fisica;

5) **«pseudonimizzazione»**: il trattamento dei dati personali in modo tale che i dati personali non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, a condizione che tali informazioni aggiuntive siano conservate separatamente e soggette a misure tecniche e organizzative intese a garantire che tali dati personali non siano attribuiti a una persona fisica identificata o identificabile;

6) **«archivio»**: qualsiasi insieme strutturato di dati personali accessibili secondo criteri determinati, indipendentemente dal fatto che tale insieme sia centralizzato, decentralizzato o ripartito in modo funzionale o geografico;

7) **«titolare del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali; quando le finalità e i mezzi di tale trattamento sono determinati dal diritto dell'Unione o degli Stati membri, il titolare

del trattamento o i criteri specifici applicabili alla sua designazione possono essere stabiliti dal diritto dell'Unione o degli Stati membri;

8) **«responsabile del trattamento»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento;

9) **«destinatario»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi. Tuttavia, le autorità pubbliche che possono ricevere comunicazione di dati personali nell'ambito di una specifica indagine conformemente al diritto dell'Unione o degli Stati membri non sono considerate destinatari; il trattamento di tali dati da parte di dette autorità pubbliche è conforme alle norme applicabili in materia di protezione dei dati secondo le finalità del trattamento;

10) **«terzo»**: la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile;

11) **«consenso dell'interessato»**: qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento;

12) **«violazione dei dati personali»**: la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati;

13) **«dati genetici»**: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico della persona fisica in questione;

14) **«dati biometrici»**: i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

15) **«dati relativi alla salute»**: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute;

16) **«stabilimento principale»**:

a) per quanto riguarda un titolare del trattamento con stabilimenti in più di uno Stato membro, il luogo della sua amministrazione centrale nell'Unione, salvo che le decisioni sulle finalità e i mezzi del trattamento di dati personali siano adottate in un altro stabilimento del titolare del trattamento nell'Unione e che quest'ultimo stabilimento abbia facoltà di ordinare l'esecuzione di tali decisioni, nel qual caso lo stabilimento che ha adottato siffatte decisioni è considerato essere lo stabilimento principale;

b) con riferimento a un responsabile del trattamento con stabilimenti in più di uno Stato membro, il luogo in cui ha sede la sua amministrazione centrale nell'Unione o, se il responsabile del trattamento non ha un'amministrazione centrale nell'Unione, lo stabilimento del responsabile del trattamento nell'Unione in cui sono condotte le principali attività di trattamento nel contesto delle attività di uno stabilimento del responsabile del trattamento nella misura in cui tale responsabile è soggetto a obblighi specifici ai sensi del presente regolamento;

17) **«rappresentante»**: la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare del trattamento o dal responsabile del trattamento per iscritto ai sensi dell'articolo 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento;

18) **«impresa»**: la persona fisica o giuridica, indipendentemente dalla forma giuridica rivestita, che eserciti un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica;

19) **«gruppo imprenditoriale»**: un gruppo costituito da un'impresa controllante e dalle imprese da questa controllate;

20) **«norme vincolanti d'impresa»**: le politiche in materia di protezione dei dati personali applicate da un titolare del trattamento o responsabile del trattamento stabilito nel territorio di uno Stato membro al trasferimento o al complesso di trasferimenti di dati personali a un titolare del trattamento o responsabile del trattamento in uno o più paesi terzi, nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune;

21) **«autorità di controllo»**: l'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'articolo 51;

22) **«autorità di controllo interessata»**: un'autorità di controllo interessata dal trattamento di dati personali in quanto:

a) il titolare del trattamento o il responsabile del trattamento è stabilito sul territorio dello Stato membro di tale autorità di controllo;

b) gli interessati che risiedono nello Stato membro dell'autorità di controllo sono o sono probabilmente influenzati in modo sostanziale dal trattamento; oppure

c) un reclamo è stato proposto a tale autorità di controllo;

23) **«trattamento transfrontaliero»**:

a) trattamento di dati personali che ha luogo nell'ambito delle attività di stabilimenti in più di uno Stato membro di un titolare del trattamento o responsabile del trattamento nell'Unione ove il titolare del trattamento o il responsabile del trattamento siano stabiliti in più di uno Stato membro; oppure

b) trattamento di dati personali che ha luogo nell'ambito delle attività di un unico stabilimento di un titolare del trattamento o responsabile del trattamento nell'Unione, ma che incide o probabilmente incide in modo sostanziale su interessati in più di uno Stato membro;

24) **«obiezione pertinente e motivata»**: un'obiezione al progetto di decisione sul fatto che vi sia o meno una violazione del presente regolamento, oppure che l'azione prevista in relazione al titolare del trattamento o responsabile del trattamento sia conforme al presente regolamento, la quale obiezione dimostra chiaramente la rilevanza dei rischi posti dal progetto di decisione riguardo ai diritti e alle libertà fondamentali degli interessati e, ove applicabile, alla libera circolazione dei dati personali all'interno dell'Unione;

25) **«servizio della società dell'informazione»**: il servizio definito all'articolo 1, paragrafo 1, lettera b), della direttiva (UE) 2015/1535 del Parlamento europeo e del Consiglio ([19]);

26) **«organizzazione internazionale»**: un'organizzazione e gli organismi di diritto internazionale pubblico a essa subordinati o qualsiasi altro organismo istituito da o sulla base di un accordo tra due o più Stati.

Art. 2 - Motivazione e obiettivo del presente Regolamento

Il riutilizzo o lo smaltimento di apparecchiature elettroniche (es. Personal Computer, Server, palmari, tablet-PC etc.) e di supporti di memorizzazione (es. hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD etc.) sono attività estremamente critiche dal punto di vista della sicurezza e della privacy dei dati personali, che devono pertanto essere rigidamente disciplinate.

Accade talvolta infatti che i dati del precedente utilizzatore – in alcuni casi estremamente riservati e delicati - non siano adeguatamente cancellati, e vengano pertanto portati a conoscenza di soggetti terzi non autorizzati; tra i casi più eclatanti che si sono verificati in tempi recenti possiamo evidenziare:

- il rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;
- il rinvenimento da parte dell'acquirente di un personal computer usato di decine di files e cartelle relativi alle patologie dei pazienti di una struttura sanitaria pubblica.

Obiettivo del presente regolamento è pertanto assicurare che il riutilizzo o lo smaltimento di apparecchiature elettroniche e di supporti di memorizzazione avvengano in condizioni di sicurezza, con la ragionevole certezza che i dati (personali, sensibili, giudiziari, di qualsiasi tipo) precedentemente memorizzati siano completamente cancellati con modalità tecniche che ne rendano impossibile il recupero.

E' infatti noto che la semplice operazione di cancellazione di in file o di una cartella, seguita dallo "svuotamento del cestino" (in ambiente Windows) non comporta la cancellazione fisica dei dati dal supporto di memorizzazione, che possono quindi essere recuperati con una certa semplicità.

E' pertanto necessario l'utilizzo di programmi di tipo "file wiping" o "file shredding", che comportano la riscrittura dei dati cancellati da sette a trentacinque volte, oppure l'utilizzo di apparati che comportino la smagnetizzazione ("degaussing") dei supporti di memorizzazione.

Art. 3 - Ambito di validità e di applicazione del presente Regolamento

Le prescrizioni del presente regolamento si applicano alle seguenti apparecchiature dell'Istituto:

- apparati di tipo "personal computer" fissi o portatili
- apparati di tipo tablet PC
- apparati di tipo server
- supporti di memorizzazione di massa, come ad esempio hard disk interni, hard disk esterni, cd-rom, dvd, chiavette usb, schede SD

e più in generale a qualsiasi apparato o dispositivo che possa contenere al suo interno qualsiasi tipo di dato (generico, personale, sensibile, giudiziario etc.).

Art. 4- Responsabilità penale e civile

Dall'inosservanza delle disposizioni contenute nel presente regolamento possono derivare responsabilità di tipo:

- amministrativo pecuniario, fino a 20.000.000,00 Euro, ai sensi dell'art. 83 del GDPR, ed eventualmente
- civile, in caso di danni cagionati a terzi, ai sensi dell'art. 82 del GDPR e dell'art. 2050 del Codice Civile.

Art. 5 - Modalità tecniche per la gestione del riutilizzo

In caso di riutilizzo di apparecchiature elettroniche o di supporti di memorizzazione, si dovranno utilizzare appositi programmi di "file wiping" o di "file shredding" che forniscano idonee garanzie di non recuperabilità dei dati cancellati, nemmeno con le apparecchiature più sofisticate.

Sul mercato esistono varie soluzioni software, alcune delle quali di pubblico dominio. Allo stato attuale della tecnologia i programmi di file wiping più affidabili sono i seguenti:

- ***Sdelete***, scaricabile dal sito www.microsoft .com, che è l'utility suggerita dalla Microdoft per tutti i sistemi Windows. Tale utility è conforme ai requisiti dello standard del DOD – Department Of Defense 5220.22-M, e fornisce idonee garanzie che I dati saranno cancellati in modo da renderne tecnicamente impossibile il recupero;
- ***Ashampoo File Wiper***, scaricabile dal sito internet www.ashampoo.it, una tra le utility più diffuse ed affidabili allo stato attuale della tecnologia.

Art. 6 - Modalità tecniche per la gestione dello smaltimento

Per lo smaltimento degli apparati e dei supporti di memorizzazione, si dovrà distinguere tra il caso in cui il dispositivo sia ancora funzionante, dai casi in cui il dispositivo non sia funzionante.

Nel primo caso si potranno applicare le modalità tecniche previste per il riutilizzo; nel secondo caso, e cioè nel caso in cui il dispositivo non sia funzionante si dovranno adottare le seguenti tecniche:

- ***Demagnetizzazione****:* la demagnetizzazione ("degaussing") permette l'"azzeramento" delle aree magnetiche delle superfici dei dischi o di altre memorie a stato solido, agendo anche sui circuiti che fanno parte del dispositivo e causandone l'inutilizzabilità successiva.
- ***Distruzione fisica***: In determinati casi è necessario ricorrrere alla distruzione fisica dei dispositivi di memoria. Tale procedura è l'unica praticabile con i supporti ottici a sola lettura (CD-ROM, DVD-R), che possono essere distrutti o polverizzati con apposite macchine analoghe ai "tritacarta" in uso negli uffici. Gli hard-disk possono essere resi inutilizzabili aprendone l'involucro protettivo e danneggiando meccanicamente le superifici magnetiche (piatti) con l'azione deformante di uno strumento o con appositi punzonatori.

Art. 7 - Autorizzazione preliminare alla cancellazione dei dati

Poiché i dati (personali, sensibili, giudiziari etc.) contenuti negli apparati e nei supporti di memorizzazione costituiscono un prezioso patrimonio dell'Istituto, e tenuto conto del fatto che in alcuni casi vi possono essere obblighi specifici di conservazione dei dati per un periodo minimo, prima di procedere alla cancellazione dei dati, chiunque sia il soggetto che materialmente effettua la cancellazione, dovrà chiedere ed ottenere in forma scritta l'autorizzazione alla cancellazione dei dati.

Detta autorizzazione dovrà essere rilasciata in forma scritta dal Dirigente Scolastico o dal DSGA. Se del caso, detta autorizzazione potrà contenere indicazioni sui dati che prima di essere cancellati devono essere oggetto di salvataggio.

Art. 8 – Verbale di corretta esecuzione della cancellazione dei dati

Alla fine delle attività di cancellazione, il soggetto che ha materialmente effettuato le operazioni dovrà compilare apposito verbale nel quale dichiara di aver personalmente effettuato la cancellazione in forma permanente dei dati e il buon esito delle operazioni effettuate.

Il suddetto verbale dovrà inoltre contenere i riferimenti (es. marca, modello, numero di serie etc.) dell'apparato o del supporto oggetto del trattamento.

Art. 9 – Soggetti tenuti alla verifica del presente regolamento

La responsabilità di vigilare sulla corretta applicazione del presente Regolamento è affidata al DPO – Data Protection Officer (Responsabile della protezione dei dati personali) dell'Istituto.

La presente delibera è stata assunta all'UNANIMITA' (11 favorevoli, 0 contrari, 0 astenuti su 11 presenti) dei voti espressi per scrutinio PALESE ed ha validità fino alla sua revoca e/o modifica.

Avverso la presente deliberazione ai sensi dell'art. 14, comma 7 del Regolamento n. 275/99 è ammesso reclamo allo stesso Consiglio entro il termine di 15 giorni dalla data di pubblicazione all'albo della scuola. Decorso tale termine la deliberazione è definitiva e contro di essa è esperibile ricorso giurisdizionale al TAR ovvero ricorso straordinario al Capo dello Stato entro il termine rispettivamente di 60 e 120 giorni dalla data di pubblicazione.

La presente delibera è stata assunta all'UNANIMITA' (11 favorevoli, 0 contrari, 0 astenuti su 11 presenti) dei voti espressi per scrutinio PALESE ed ha validità fino alla sua revoca e/o modifica.

F.to Il Segretario
(prof. Luciano Gonano)

F.to Il Presidente
(Sig. Costanzo Nevio)

Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3 comma 2, del D.Lgs. 39/93

Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3 comma 2, del D.Lgs. 39/93

La presente delibera è copia conforme all'originale.

Gorizia, il (vedasi data pubblicazione albo on line)

F.to IL DIRIGENTE SCOLASTICO REGGENTE
(Prof.ssa Rizzatto Rossella)
Firma autografa sostituita a mezzo stampa
ai sensi dell'art. 3 comma 2, del D.Lgs. 39/93
