

2020

Liceo Michelangiolo Regolamento applicativo GDPR



Preside

Sommario

PARTE PRIMA: INTRODUZIONE	4
PREMESSA DI CARATTERE NORMATIVO	4
PREMESSA DI CARATTERE ORGANIZZATIVO	5
PREMESSA DI CARATTERE METODOLOGICO	6
PARTE SECONDA DISPOSIZIONI GENERALI	7
OGGETTO DEL REGOLAMENTO	7
FINALITÀ' DEL REGOLAMENTO	7
SENSIBILIZZAZIONE	7
DEFINIZIONI	8
PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI	10
TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)	10
TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)	11
COMUNICAZIONE DI DATI VERSO L'ESTERNO	11
PARTE TERZA DIRITTI DELL'INTERESSATO	12
INFORMATIVA SUL TRATTAMENTO DEI DATI	12
CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI	13
DIRITTO DI ACCESSO DELL'INTERESSATO	20
DIRITTO DI RETTIFICA	23
DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)	23
DIRITTO DI LIMITAZIONE AL TRATTAMENTO	24
DIRITTO ALLA PORTABILITÀ' DEI DATI	24
DIRITTO DI OPPOSIZIONE	24
PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)	25
PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO	26
TITOLARE DEL TRATTAMENTO	26
CONTITOLARI DEL TRATTAMENTO	27
RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI	27
RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI	29
AUTORIZZATO INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI	31
RESPONSABILE DELLA PROTEZIONE DEI DATI	31
PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO	34
PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA	34
REGISTRO ELETTRONICO DELLE ATTIVITÀ' DI TRATTAMENTO	34
PROTEZIONE E SICUREZZA DEI DATI PERSONALI	34
NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITÀ' DI CONTROLLO	35
VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI	36

TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO	36
DISCIPLINA SULLA VIDEOSORVEGLIANZA	36
DISCIPLINA SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI	36
PARTE SESTA ATTUAZIONE IN AMBITO SCOLASTICO DEGLI ADEMPIMENTI EUROPEI	40
AMBITI DI ATTIVITA' CORRELATI AI NUOVI OBBLIGHI EUROPEI	40
ENTRATA IN VIGORE E PUBBLICITA'	41
DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'	41

PARTE PRIMA: INTRODUZIONE

PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento in materia di protezione dei dati personali è uno strumento per l'applicazione del nuovo **Regolamento UE n. 2016/679 (GDPR)**, nell'ambito dell'organizzazione del Liceo classico statale Michelangiolo.

Il Regolamento UE, in vigore dal 25.05.2018, disciplina la protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché la libera circolazione di tali dati. Esso abroga la precedente Direttiva 95/46/CE.

Le disposizioni legislative nazionali del Codice in materia di protezione dei dati personali *D.lgs. 196/2003 e ss.mm.ii.*, sono state novellate dal Decreto legislativo 10 agosto 2018, n. 101 che adegua il suddetto Codice alle disposizioni del Regolamento (UE) 2016/679.

Il presente Regolamento applicativo è sottoposto ad aggiornamento periodico, in linea con le novità normative, giurisprudenziali e con le pronunce del Garante per la protezione dei dati personali.

PREMESSA DI CARATTERE ORGANIZZATIVO

Il corretto trattamento dei dati personali è da considerarsi non un oneroso rispetto di adempimenti burocratici ma una indispensabile garanzia per il cittadino che utilizzi un qualsiasi servizio, specialmente se questo venga offerto da una istituzione pubblica come un Liceo statale.

Il diritto al corretto trattamento dei dati personali costituisce, secondo il Legislatore europeo, un diritto inviolabile dell'essere umano, che attiene al rispetto delle libertà fondamentali e della dignità del singolo individuo.

Il corretto trattamento dei dati personali è un elemento cardine dell'organizzazione di questo Liceo, che si impegna perché tale cultura possa crescere e rafforzarsi fra gli tutti gli operatori, in quanto solo con la conoscenza dei principi fondamentali alla base della vigente normativa si possono correttamente attuare tutte le azioni di carattere tecnico e organizzativo progettate.

Link di interesse

www.liceomichelangiolo.it

www.garanteprivacy.it

www.liceomichelangiolo.it/index.php/privacy-dpo

Ai sensi del Regolamento UE679/2016 (GDPR), si comunicano i dati di riferimento dei referenti e si rinvia alla pagina del sito istituzionale dove è pubblicata l'informativa completa. Qualsiasi approfondimento può essere svolto sul sito del garante al seguente indirizzo www.garanteprivacy.it

Titolare del trattamento: Istituto "Liceo classico Michelangiolo" rappresentato dal dirigente scolastico dott.ssa Gilda Tortora	Numero di telefono: 0552478151 Indirizzo email: fipc004000n@istruzione.it
Responsabile Protezione Dati (RPD): ing. Angelo Zerella	Indirizzo email: angelo.zerella@gmail.com

PREMESSA DI CARATTERE METODOLOGICO

A questo Regolamento applicativo si allegano i **documenti tecnici** necessari a dare compiuta attuazione, sia verso l'interno che verso l'esterno, GDPR. Tali documenti sono pubblicati sul sito web istituzionale nella sezione privacy.

Principio introdotto dal GDPR è la “**responsabilizzazione**” (*accountability*) che pone in carico al Titolare del trattamento dei dati l'obbligo di definire misure tecniche e organizzative adeguate in materia di protezione dei dati, per assicurare la “**conformità**” (*compliance*); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare la piena e corretta applicazione del GDPR.

Il Liceo Michelangiolo ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* e alla *compliance*.

PARTE SECONDA DISPOSIZIONI GENERALI

OGGETTO DEL REGOLAMENTO

Il presente Regolamento applicativo del GDPR - Liceo Michelangiolo descrive le modalità attuative definite per assicurare il corretto trattamento dei dati personali.

FINALITÀ' DEL REGOLAMENTO

Il Liceo Michelangiolo si impegna a garantire che il trattamento di dati personali si svolga unicamente quando sussistano i presupposti che lo rendono lecito, art. 6 GDPR.

La protezione delle persone fisiche, con riguardo al trattamento dei dati personali, è un diritto fondamentale. Ogni persona ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della *Carta dei diritti fondamentali UE*)

SENSIBILIZZAZIONE

Il Liceo Michelangiolo sostiene e promuove ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

A tale riguardo, uno degli strumenti essenziali di sensibilizzazione in materia di corretto trattamento dei dati personali, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con la Scuola.

Per garantire la conoscenza adeguata delle disposizioni introdotte dal GDPR, e del presente Regolamento Applicativo, al momento dell'ingresso in servizio è fornita, a cura della Segreteria del Personale, ad ogni dipendente (*oltre che ad ogni collaboratore, consulente, esperto esterno*) una specificata comunicazione in materia di trattamento di dati personali, con eventuale nomina di “**autorizzato al trattamento dei dati**” ai sensi del Regolamento UE 2016/679.

Detta comunicazione conterrà anche i riferimenti per reperire il presente Regolamento Applicativo sul sito internet.

DEFINIZIONI

Dall' art. 4 del GDPR, si riportano alcune definizioni.

a) «**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;

b) «**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;

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

d) «**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;

e) «**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;

f) «**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;

g) «**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;

h) «**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;

i) «**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;

l) «**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;

m) «**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;

n) «**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;

o) «**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;

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

PRINCIPI APPLICABILI AL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 5 del GDPR, i dati personali sono:

a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («**liceità, correttezza e trasparenza**»);

b) raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1 del GDPR, considerato incompatibile con le finalità iniziali («**limitazione della finalità**»);

c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («**minimizzazione dei dati**»).

d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («**esattezza**»);

e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1 del Regolamento UE, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («**limitazione della conservazione**»);

f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («**integrità e riservatezza**»).

Come stabilito dal Regolamento UE, il Titolare del trattamento (Scuola nella persona del

Dirigente Scolastico della Scuola) è competente per il rispetto di quanto sin qui esposto ed è in grado di comprovarlo verso l'esterno (principio europeo dell'«**accountability**» o «**responsabilizzazione**»).

TRATTAMENTO DI CATEGORIE PARTICOLARI DI DATI (DATI SENSIBILI)

Come stabilito dall'articolo n. 9 del Regolamento Europeo n. 2016/679, è vietato trattare dati personali che rivelino l'*origine razziale o etnica*, le *opinioni politiche*, le *convinzioni religiose o filosofiche*, o l'*appartenenza sindacale*, nonché trattare *dati genetici*, *dati biometrici* intesi a identificare in modo univoco una persona fisica, *dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona*.

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati sensibili, biometrici e genetici e in particolare con le «*Autorizzazioni generali*», dall'Autorità Garante per la protezione di dati personali.

TRATTAMENTO DEI DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI (DATI GIUDIZIARI)

Come stabilito dall'articolo n. 10 del GDPR, «*il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica.*»

Posto quanto sopra, si fa rinvio alle vigenti disposizioni emanate, in materia di dati giudiziari e in particolare con le «*Autorizzazioni generali*», dall'Autorità Garante per la protezione di dati personali.

COMUNICAZIONE DI DATI VERSO L'ESTERNO

La **comunicazione di dati sensibili e giudiziari da parte di un soggetto pubblico ad altro soggetto pubblico** è ammessa quando è prevista da una norma di legge o regolamento e comunque quando è ritenuta necessaria per lo svolgimento di funzioni istituzionali, anche a seguito di un bilanciamento degli interessi in gioco.

PARTE TERZA DIRITTI DELL'INTERESSATO

INFORMATIVA SUL TRATTAMENTO DEI DATI

Come stabilito dall'articolo n. 13 del GDPR, in caso di raccolta presso l'interessato di dati che lo riguardano, il Titolare del trattamento fornisce all'interessato, nel momento in cui i dati personali sono ottenuti, le seguenti **informazioni**:

- a) l'identità e i dati di contatto del titolare del trattamento e, ove applicabile, del suo rappresentante;
- b) i dati di contatto del Responsabile della protezione dei dati (D.P.O.);
- c) le finalità del trattamento cui sono destinati i dati personali nonché la base giuridica del trattamento;
- d) qualora il trattamento si basi sull'articolo 6, paragrafo 1, lettera f) del Regolamento UE, i legittimi interessi perseguiti dal titolare del trattamento o da terzi;
- e) gli eventuali destinatari o le eventuali categorie di destinatari dei dati personali;
- f) ove applicabile, l'intenzione del titolare del trattamento di trasferire dati personali a un paese terzo o a un'organizzazione internazionale e l'esistenza o l'assenza di una decisione di adeguatezza della Commissione, nei termini previsti dal Regolamento UE.

In aggiunta alle informazioni di cui sopra, nel momento in cui i dati personali sono ottenuti, il titolare del trattamento fornisce all'interessato le seguenti **ulteriori informazioni necessarie** per garantire un trattamento corretto e trasparente:

- a) il periodo di conservazione dei dati personali oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- b) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano o di opporsi al loro trattamento, oltre al *diritto alla portabilità* dei dati;
- c) qualora il trattamento sia basato sull'articolo 6, paragrafo 1, lettera a), oppure sull'articolo 9, paragrafo 2, lettera a) del Regolamento UE, l'esistenza del diritto di revocare il consenso in qualsiasi momento senza pregiudicare la liceità del trattamento basata sul consenso prestato prima della revoca;
- d) il diritto di proporre reclamo a un'autorità di controllo;
- e) se la comunicazione di dati personali è un obbligo legale o contrattuale oppure un requisito necessario per la conclusione di un contratto, e se l'interessato ha l'obbligo di fornire i dati personali nonché le possibili conseguenze della mancata comunicazione di tali dati;
- f) l'eventuale esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4 del Regolamento UE, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Per quanto concerne il periodo di conservazione dei dati personali raccolti da questa SCUOLA, i dati verranno conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello strettamente necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

Qualora il Titolare del trattamento intenda trattare ulteriormente i dati personali per una **finalità** diversa da quella per cui essi sono stati raccolti, prima di tale ulteriore trattamento fornisce all'interessato informazioni in merito a tale diversa finalità.

Per l'applicazione di quanto su esposto, si rinvia alla Guida all'informativa privacy Michelangiolo, ove sono raccolti sia i modelli di **"Informativa"** sia un modulo generico per la raccolta del **"consenso"**, da personalizzare in relazione agli eventi specifici.

CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il GDPR stabilisce che ogni trattamento deve trovare fondamento in un'ideale base giuridica; i fondamenti di **liceità del trattamento** sono indicati all'art. 6 del Regolamento: *consenso, adempimento obblighi contrattuali, interessi vitali della persona interessata o di terzi, obblighi di legge cui è soggetto il titolare, interesse pubblico o esercizio di pubblici poteri, interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.*

In particolare:

- **per i dati "sensibili" il consenso deve essere "esplicito"** (si veda art. 9 regolamento): lo stesso dicasi per il consenso a decisioni basate su **trattamenti automatizzati** (compresa la profilazione, articolo 22);
- **non deve essere necessariamente "documentato per iscritto"**, né è richiesta la "forma scritta", anche se questa è modalità idonea a configurare inequivocabile accettazione del consenso e il suo essere "esplicito" (per i dati sensibili); inoltre, il Titolare deve essere in grado di dimostrare che l'interessato ha prestato il consenso a uno specifico trattamento;
- Il **consenso dei minori** è valido a partire dai 16 anni: prima di tale età occorre raccogliere il consenso di chi esercita la responsabilità genitoriale (articolo n. 8 del GDPR); qualora non sia inteso (il consenso) come raccolta per utilizzo di strumenti dell'informazione (es. Google app, registri elettronici, social, etc.) allora lo stesso può essere anche raccolto solo per i minori di 14 anni.

- deve essere, in tutti i casi, **libero, specifico, informato e inequivocabile** e non è ammesso il consenso tacito o presunto (non è quindi possibile utilizzare “caselle pre-spuntate” su un modulo);
- deve essere manifestato attraverso “**dichiarazione o azione positiva inequivocabile**” (per approfondimenti, si vedano considerando 39 e 42 del regolamento).

Interesse vitale di un terzo: si può invocare tale base giuridica solo se nessuna delle altre condizioni di liceità può trovare applicazione (si veda considerando 46 del GDPR).

Interesse legittimo prevalente di un titolare o di un terzo:

- Il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell'interessato non spetta all'Autorità ma è compito dello stesso Titolare; si tratta di una delle principali espressioni del **principio di “responsabilizzazione”** introdotto dal nuovo pacchetto protezione dati;
- l'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire un valido fondamento di liceità;
- il regolamento chiarisce espressamente che l'interesse legittimo del titolare non costituisce idonea base giuridica per i trattamenti svolti dalle autorità pubbliche in esecuzione dei rispettivi compiti.

DIRITTO DI ACCESSO DELL'INTERESSATO

Come stabilito dall'articolo n. 15 del GDPR, l'interessato ha il diritto di ottenere dal Titolare del trattamento la conferma che sia o meno in corso un trattamento di dati personali che lo riguardano e in tal caso, di ottenere **l'accesso** ai dati personali e alle seguenti informazioni:

- a) le finalità del trattamento;
- b) le categorie di dati personali in questione;
- c) i destinatari o le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, in particolare se destinatari di paesi terzi o organizzazioni internazionali;
- d) quando possibile, il periodo di conservazione dei dati personali previsto oppure, se non è possibile, i criteri utilizzati per determinare tale periodo;
- e) l'esistenza del diritto dell'interessato di chiedere al titolare del trattamento la rettifica o la cancellazione dei dati personali o la limitazione del trattamento dei dati personali che lo riguardano o di opporsi al loro trattamento;
- f) il diritto di proporre reclamo a un'autorità di controllo;
- g) qualora i dati non siano raccolti presso l'interessato, tutte le informazioni disponibili sulla loro origine;
- h) l'esistenza di un *processo decisionale automatizzato*, compresa la *profilazione* di cui all'articolo 22, paragrafi 1 e 4, e, almeno in tali casi, informazioni significative sulla logica utilizzata, nonché l'importanza e le conseguenze previste di tale trattamento per l'interessato.

Oltre al rispetto delle prescrizioni relative alle modalità di esercizio di questo diritto, il Titolare può consentire agli interessati di consultare direttamente, da remoto e in modo sicuro, i propri dati personali.

Qualora i dati personali siano trasferiti a un paese terzo o a un'organizzazione internazionale, l'interessato ha il diritto di essere informato dell'esistenza di garanzie adeguate ai sensi dell'articolo 46 relative al trasferimento.

Il titolare del trattamento fornisce una copia dei dati personali oggetto di trattamento.

In caso di ulteriori copie richieste dall'interessato, il titolare del trattamento può addebitare un contributo spese ragionevole basato sui costi amministrativi. Se l'interessato presenta la richiesta mediante mezzi elettronici, e salvo indicazione diversa dell'interessato, le informazioni sono fornite in un formato elettronico di uso comune.

Il diritto di ottenere una copia non deve ledere i diritti e le libertà altrui.

Per l'applicazione di quanto su esposto, si rinvia alla [Guida all'informativa privacy Michelangiolo](#), ove sono raccolti sia i modelli di **"Informativa"** sia un modulo generico per la raccolta del **"consenso"**, da personalizzare in relazione agli eventi specifici.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo e organizzativo, il **diritto di accesso**, si fa rinvio alle vigenti disposizioni normative e regolamentari emanate, negli anni, dal Legislatore statale e regionale nonché dal Garante per la privacy, con particolare riferimento all'ambito scolastico.

DIRITTO DI RETTIFICA

Come stabilito dall'articolo n. 16 del GDPR, l'interessato ha il diritto di ottenere dal Titolare del trattamento la rettifica dei dati personali inesatti che lo riguardano senza ingiustificato ritardo. Tenuto conto delle finalità del trattamento, l'interessato ha il diritto di ottenere l'integrazione dei dati personali incompleti, anche fornendo una dichiarazione integrativa.

DIRITTO ALLA CANCELLAZIONE (DIRITTO ALL'OBLIO)

Come stabilito dall'articolo n. 17 del GDPR, in capo all'interessato è riconosciuto il **diritto "all'oblio"**, che si configura come un diritto alla cancellazione dei propri dati personali **in forma rafforzata**.

Si prevede, infatti, l'obbligo per i Titolari (se hanno "reso pubblici" i dati personali dell'interessato: ad esempio, pubblicandoli su un sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione" (si veda art. 17, paragrafo 2 del GDPR).

DIRITTO DI LIMITAZIONE AL TRATTAMENTO

È esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento (quale alternativa alla cancellazione dei dati stessi), bensì **anche se l'interessato chiede la rettifica dei dati** (*in attesa di tale rettifica da parte del titolare*) o **si oppone al loro trattamento ai sensi dell'art. 21 del regolamento** (*in attesa della valutazione da parte del titolare*).

Esclusa la conservazione, ogni altro trattamento del dato di cui si chiede la **limitazione** è vietato a meno che ricorrano determinate circostanze (*consenso dell'interessato, accertamento diritti in sede giudiziaria, tutela diritti di altra persona fisica o giuridica, interesse pubblico rilevante*).

Il diritto alla limitazione prevede che il dato personale sia **“contrassegnato”** in attesa di determinazioni ulteriori; pertanto, è opportuno che il Titolare preveda nei propri sistemi informativi (elettronici o meno) misure idonee a tale scopo.

DIRITTO ALLA PORTABILITA' DEI DATI

Si tratta di uno dei nuovi diritti previsti dal regolamento, anche se non è del tutto sconosciuto ai consumatori (si pensi alla portabilità del numero telefonico).

Non si applica ai trattamenti non automatizzati (quindi non si applica agli archivi o registri cartacei) e sono previste **specifiche condizioni per il suo esercizio**; in particolare, sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o sull'interesse legittimo del titolare, per esempio), e solo i dati che siano stati “forniti” dall'interessato al Titolare (si veda il considerando 68 del GDPR).

Inoltre, il Titolare deve essere in grado di trasferire direttamente i dati portabili a un altro titolare indicato dall'interessato, se tecnicamente possibile.

DIRITTO DI OPPOSIZIONE

Come stabilito dall'articolo n. 21 del GDPR, l'interessato ha il **diritto di opporsi in qualsiasi momento**, per motivi connessi alla sua situazione particolare, al trattamento dei dati personali che lo riguardano ai sensi dell'articolo 6, paragrafo 1, lettere e) o f) del medesimo Regolamento, compresa la profilazione sulla base di tali disposizioni. Il Titolare del trattamento si astiene dal trattare ulteriormente i dati personali salvo che egli dimostri l'esistenza di motivi legittimi cogenti per procedere al trattamento che prevalgono sugli interessi, sui diritti e sulle libertà dell'interessato oppure per l'accertamento, l'esercizio o la difesa di un diritto in sede giudiziaria.

PROCESSO DECISIONALE AUTOMATIZZATO (PROFILAZIONE)

Come stabilito dall'articolo n. 22 del GDPR, l'interessato ha il diritto di non essere sottoposto a una decisione basata unicamente sul **trattamento automatizzato**, compresa la

profilazione, che produca effetti giuridici che lo riguardano o che incida in modo analogo significativamente sulla sua persona.

Tale principio non si applica nel caso in cui la decisione:

- sia necessaria per la conclusione o l'esecuzione di un contratto tra l'interessato e un titolare del trattamento;
- sia autorizzata dal diritto dell'Unione o dello Stato membro cui è soggetto il titolare del trattamento, che precisa altresì misure adeguate a tutela dei diritti, delle libertà dei legittimi interessi dell'interessato;
- si basi sul consenso esplicito dell'interessato.

PARTE QUARTA TITOLARE E RESPONSABILE DEL TRATTAMENTO

TITOLARE DEL TRATTAMENTO

Il "**Titolare**" del trattamento dei dati personali è la persona fisica, giuridica, la Pubblica Amministrazione, e qualsiasi altro Ente, Associazione od organismo cui competono le decisioni in ordine alle finalità, alle modalità del trattamento di dati personali e agli strumenti utilizzati, compreso il profilo della sicurezza.

Il Titolare del trattamento dei dati personali, ai sensi e per gli effetti del vigente Codice della privacy, è la Scuola, nella persona del suo Dirigente Scolastico, in qualità di legale rappresentante del Liceo classico Michelangiolo, con sede in via della Colonna, 9.

Il Titolare provvede a:

- a) richiedere al Garante per la protezione dei dati personali l'eventuale autorizzazione al trattamento dei dati personali, nei casi previsti dalla vigente normativa e ad assolvere all'eventuale obbligo di notificazione e comunicazione;
- b) nominare con atto deliberativo i *Responsabili del trattamento dei dati personali*, impartendo ad essi, per la corretta gestione e tutela dei dati personali, i compiti e le necessarie istruzioni, in relazione all'informativa agli interessati, alla tipologia dei dati da trattare, alle condizioni normative previste per il trattamento dei dati, alle modalità di raccolta, comunicazione e diffusione dei dati, all'esercizio dei diritti dell'interessato previsti dall'art. 7 del Codice della Privacy e all'articolo 12 del Regolamento UE, all'adozione delle misure di sicurezza per la conservazione, alla protezione e sicurezza dei dati;
- c) nominare il Data Protection Officer, come stabilito dall'articolo 37 del GDPR;
- d) disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;
- e) mettere in atto misure tecniche e organizzative adeguate per garantire che il trattamento dei dati sia effettuato conformemente al presente Regolamento.

Si dà evidenza, inoltre, del fatto che il GDPR pone con forza l'accento sulla "**responsabilizzazione**" (**accountability** nell'accezione inglese) di titolari e responsabili, ovvero sulla adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento (si vedano artt. 23-25, in

particolare, e l'intero Capo IV del GDPR).

Si tratta di una grande novità per la protezione dei dati in quanto viene affidato ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative e alla luce di alcuni criteri specifici indicati nel regolamento.

Il Liceo classico Michelangiolo, nella persona del Suo Dirigente Scolastico, ha fatto proprio l'approccio del Legislatore europeo relativo all'*accountability* sin dalla adozione della Deliberazione n. 86 del 24.01.2018 relativa alle "prime azioni" utili ad ottemperare alle previsioni legislative del GDPR.

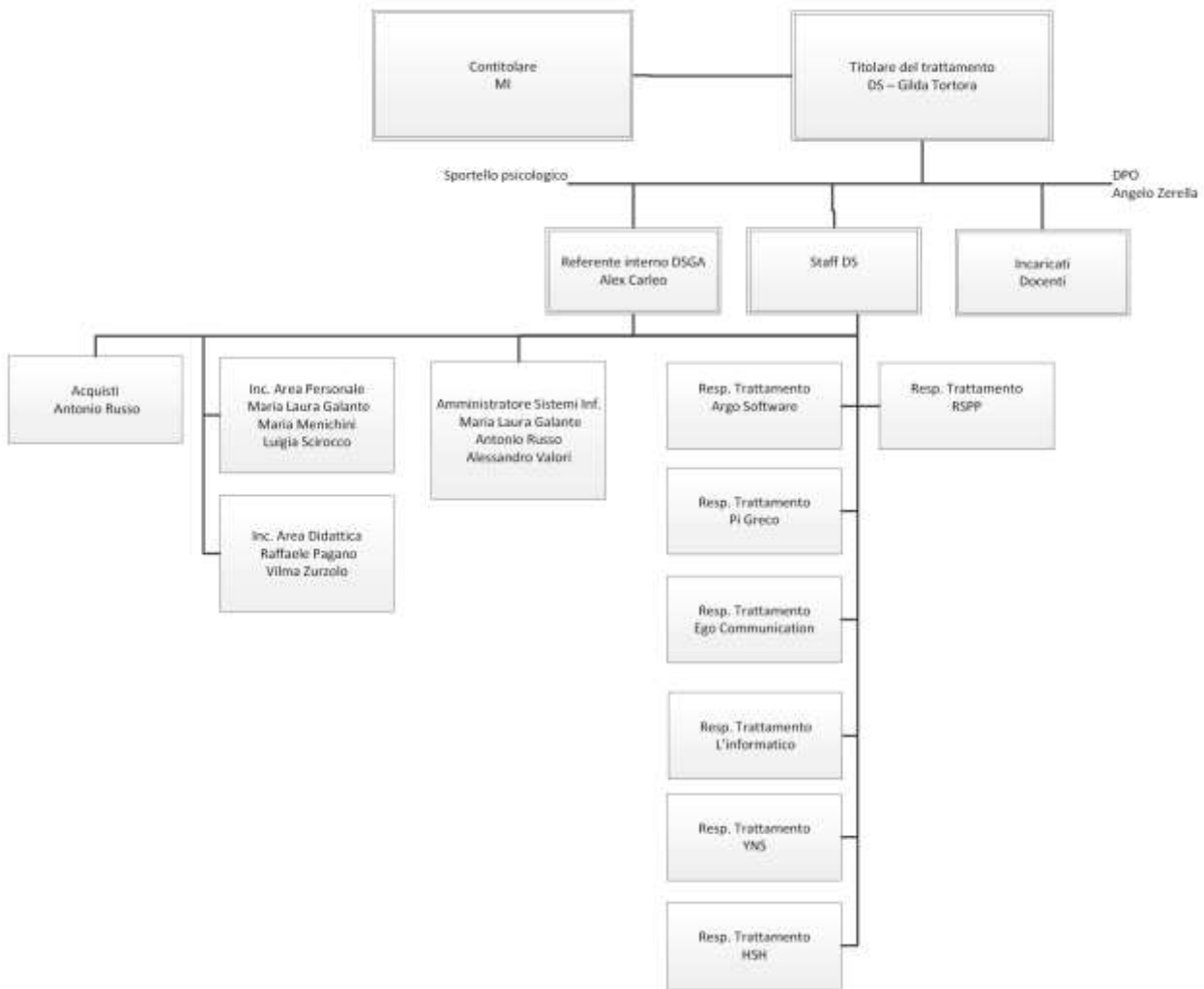
CONTITOLARI DEL TRATTAMENTO

Come stabilito dall'articolo n. 26 del GDPR, allorché due o più titolari del trattamento determinano congiuntamente le finalità e i mezzi del trattamento, essi sono **contitolari del trattamento**. Essi determinano in modo trasparente, mediante un *accordo interno*, le rispettive responsabilità in merito all'osservanza degli obblighi derivanti dal Regolamento UE, con particolare riguardo all'esercizio dei diritti dell'interessato, e le rispettive funzioni di comunicazione delle informazioni.

Tale accordo può designare un punto di contatto per gli interessati e riflette adeguatamente i rispettivi ruoli e i rapporti dei contitolari con gli interessati. Il contenuto essenziale dell'accordo è messo a disposizione dell'interessato.

Indipendentemente dalle disposizioni dell'accordo anzidetto, l'interessato può esercitare i propri diritti ai sensi del GDPR nei confronti di e contro ciascun Titolare del trattamento.

ORGANIGRAMMA LICEO MICHELANGIOLO PER IL TRATTAMENTO DEI DATI PERSONALI



Il Titolare del trattamento dei dati provvede a consegnare a ciascun ruolo indicato lettera di nomina che specifica le responsabilità, relative al trattamento dei dati personali, connesse al ruolo svolto. Ciascuno deve:

- 1) trattare i dati personali, anche sensibili, osservando le disposizioni del presente Regolamento nonché le specifiche istruzioni impartite dal Titolare;
- 2) garantire che, presso la propria struttura, le persone autorizzate (incaricate) al trattamento dei dati personali assolvano ad un adeguato livello di riservatezza;
- 3) adottare idonee misure per garantire, nell'organizzazione delle prestazioni e dei servizi presso la propria struttura, il rispetto dei diritti, delle libertà fondamentali e della dignità degli interessati, nonché del segreto professionale, fermo restando quanto previsto dalla normativa vigente;
- 4) tenendo conto della natura del trattamento, assistere il Titolare del trattamento con misure tecniche ed organizzative adeguate, al fine di soddisfare l'obbligo del Titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato secondo quanto previsto nella normativa vigente;

- 5) mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi previsti nel presente Regolamento;
- 6) contribuire alle attività di verifica del rispetto del regolamento, comprese le ispezioni, realizzate dal titolare del trattamento o da altro soggetto da questi incaricato.

Ciascuno, nell'espletamento della sua funzione, deve inoltre collaborare con il **Data Protection Officer (DPO)**:

- a) comunicando al DPO ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del GDPR riguardanti: *l'adozione di misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio; la notificazione di una violazione dei dati personali al Garante privacy; la comunicazione di una violazione dei dati personali all'interessato, la predisposizione del Registro dei trattamenti.*
- b) utilizzando i modelli di *Informativa e Consenso* approvati con il presente Regolamento, verificandone il rispetto e fornendo al DPO le informazioni utili per l'aggiornamento del registro dei trattamenti;
- c) rispondendo alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilendo modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- d) contribuendo a far sì che tutte le misure di sicurezza riguardanti i dati della Scuola siano applicate all'interno della Scuola stessa e all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
- e) informando il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

RESPONSABILI DEL TRATTAMENTO DEI DATI

Sono inoltre individuati i **Responsabili del trattamento dei dati personali**, soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto, trattino dati di cui è titolare il Liceo Michelangiolo e in possesso dei requisiti previsti dall'articolo 29 del GDPR, Tali Responsabili hanno l'obbligo di:

- trattare i dati in modo lecito, secondo correttezza e nel pieno rispetto della vigente normativa (nazionale ed europea) in materia di privacy;
- trattare i dati personali, anche di natura sensibile e giudiziaria, degli studenti (o di altri interessati) esclusivamente per le finalità previste dal contratto o dalla convenzione stipulata con la SCUOLA e ottemperando ai principi generali di necessità, pertinenza e non eccedenza;
- rispettare i principi in materia di sicurezza dettati dalla normativa vigente (nazionale ed europea) in materia di privacy, idonei a prevenire e/o evitare operazioni di comunicazione o diffusione dei dati non consentite, il rischio di distruzione o perdita, anche accidentale, il rischio di accesso non autorizzato o di trattamento non autorizzato o non conforme alle finalità della raccolta;

- adottare, secondo la propria organizzazione interna, misure tecniche ed organizzative idonee a garantire un livello di sicurezza adeguato al rischio, nei termini di cui all'articolo 32 del GDPR, "Sicurezza del trattamento";
- nominare, al loro interno, i soggetti autorizzati / incaricati del trattamento, impartendo loro tutte le necessarie istruzioni finalizzate a garantire, da parte degli stessi, un adeguato obbligo legale di riservatezza;
- attenersi alle disposizioni impartite dal Titolare del trattamento, anche nell'eventuale caso di trasferimento di dati personali verso un paese terzo o un'organizzazione internazionale, nei termini di cui all'articolo 28, comma 3, lettera a) del Regolamento Europeo;
- specificare, su richiesta del Titolare, i luoghi dove fisicamente avviene il trattamento dei dati e su quali supporti e le misure minime di sicurezza adottate per garantire la riservatezza e la protezione dei dati personali trattati.
- assistere, per quanto di competenza e nella misura in cui ciò sia possibile, il Titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36 del Regolamento Europeo (*sicurezza del trattamento dei dati personali, notifica di una violazione dei dati personali all'autorità di controllo, comunicazione di una violazione dei dati personali all'interessato, valutazione di impatto sulla protezione dei dati*), tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento;
- su scelta del Titolare del trattamento, cancellare o restituire al medesimo tutti i dati personali dopo che è terminata la prestazione dei servizi relativi al trattamento e cancellare le copie esistenti, salvo che il diritto dell'Unione o dello Stato membro preveda la conservazione dei dati;
- mettere a disposizione del Titolare del trattamento tutte le informazioni necessarie per dimostrare il rispetto degli obblighi di cui all'articolo 28 del Regolamento Europeo e consentire e contribuire alle attività di revisione, comprese le ispezioni, realizzate dal Titolare del trattamento o da un altro soggetto da questi incaricato.

Nel caso di mancato rispetto delle predette disposizioni e in caso di mancata nomina dei soggetti incaricati al trattamento dei dati ne risponde direttamente, verso la Scuola, il Responsabile Esterno del trattamento.

La designazione del Responsabile esterno viene effettuata mediante "accordo di nomina" sottoscritto da parte del Titolare del trattamento e controfirmato per accettazione da parte del Responsabile esterno: il documento deve essere richiamato dagli accordi, convenzioni o contratti che prevedono l'affidamento di trattamenti di dati personali esternamente alla Scuola.

In allegato al presente Regolamento sono le nomine ai Responsabili.

L'accettazione della nomina e l'impegno a rispettare le disposizioni del presente Regolamento è condizione necessaria per l'instaurarsi del rapporto giuridico fra le Parti.

AUTORIZZATO INTERNO ED ESTERNO DEL TRATTAMENTO DEI DATI

Il GDPR stabilisce che chi tratta dati personali, ricevendo istruzioni e formazione da parte del Titolare del trattamento, debba da questi essere “*autorizzato*” al trattamento (articoli 4 e 10 del GDPR).

Ci si riferisce, a titolo esemplificativo, al *personale tirocinante* o al *personale volontario* che opera temporaneamente all'interno della Scuola in virtù di un accordo o di una convenzione con un Ente esterno pubblico o privato (es. Associazione di volontariato o Ente universitario) per lo svolgimento, appunto, di tirocini formativi piuttosto che di attività di volontariato o di sostegno.

Nel caso di autorizzati esterni, l'accesso ai dati deve essere limitato, con particolare rigore, ai soli dati personali la cui conoscenza sia strettamente necessaria per l'adempimento dei compiti assegnati e connessi all'espletamento dell'attività.

RESPONSABILE DELLA PROTEZIONE DEI DATI

Il Regolamento Europeo impone la nomina del **Data Protection Officer** (in italiano: Responsabile della protezione dei dati o 'RDP'), nei termini di cui all'articolo 37, 38 e 39 del Regolamento medesimo.

La nomina del DPO è obbligatoria in tutte le organizzazioni pubbliche.

Chi svolge la funzione di DPO, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. E non avere **conflitti di interessi**.

Ai sensi dell'articolo 39 del GDPR, i suoi compiti sono:

- ✓ **sorvegliare l'osservanza del Regolamento**, valutando i rischi di ogni trattamento alla luce della natura, dell'ambito di applicazione e delle finalità;
- ✓ **fornire consulenza e pareri** al Titolare, ai Responsabili del trattamento dei dati e agli incaricati relativamente all'applicazione degli obblighi europei in materia;
- ✓ collaborare con il titolare, laddove necessario, nel condurre una **valutazione di impatto sulla protezione dei dati (DPIA)**;
- ✓ **informare e sensibilizzare** il titolare o il responsabile del trattamento, nonché i dipendenti di questi ultimi, riguardo agli obblighi derivanti dal regolamento e da altre disposizioni in materia di protezione dei dati;
- ✓ **cooperare con il Garante e fungere da punto di contatto per il Garante** su ogni questione connessa al trattamento;
- ✓ **supportare** il titolare o il responsabile in ogni attività connessa al trattamento di dati personali, anche con riguardo alla tenuta di un **registro delle attività di trattamento**.

Ai sensi dell'articolo 37 del GDPR, il DPO deve:

1. **possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali**, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad

appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze;

2. **adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.** In linea di principio, ciò significa che il RPD non può essere un soggetto che ricopre ruoli gestionali e che decide sulle finalità o sugli strumenti del trattamento di dati personali;
3. operare alle dipendenze del titolare oppure sulla base di un contratto di servizio (DPO esterno);
4. **disporre di risorse umane e finanziarie**, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il GDPR prevede la pubblicazione *on line* del curriculum del DPO, nonché la pubblicazione sul sito istituzionale dell'Ente dei **“dati di contatto” del DPO**: dati che debbono essere inseriti anche nell'informativa sul trattamento dei dati, così che il DPO sia agevolmente contattabile dai cittadini-utenti e dal Garante per la privacy.

PARTE QUINTA: SICUREZZA DEI DATI PERSONALI MISURE DI CARATTERE INFORMATICO E TECNOLOGICO

PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PROTEZIONE PER IMPOSTAZIONE PREDEFINITA

L'articolo n. 25 del GDPR introduce il criterio sintetizzato dall'espressione inglese **“data protection by default and by design”**, ossia dalla necessità di configurare il trattamento prevedendo fin dall'inizio le garanzie indispensabili al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati, tenendo conto del contesto complessivo ove il trattamento si colloca e dei rischi per i diritti e le libertà degli interessati.

Tutto questo deve avvenire a monte, prima di procedere al trattamento dei dati vero e proprio (*“sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso”*, secondo quanto afferma l'art. 25, paragrafo 1 del GDPR) e richiede, pertanto, un'analisi preventiva ed un impegno applicativo da parte del Titolare che deve sostanziarsi in una serie di attività specifiche e dimostrabili.

REGISTRO ELETTRONICO DELLE ATTIVITA' DI TRATTAMENTO

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti ma solo se non effettuano trattamenti a rischio (si veda l'articolo 30, paragrafo 5 del GDPR), devono tenere un **registro delle operazioni di trattamento** i cui contenuti sono indicati all'articolo 30 del medesimo Regolamento.

Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o di un soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio.

Il Registro, in virtù delle dimensioni e della complessità che caratterizzano questa SCUOLA verrà gestito in via digitale e sarà esibito su richiesta del Garante.

La tenuta del registro elettronico dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema tecnologico di corretta gestione dei dati personali.

Per tale motivo, anche questa SCUOLA, per mezzo dei competenti servizi dell'area informatica, è impegnata a compiere i passi necessari per gestire tale registro elettronico.

PROTEZIONE E SICUREZZA DEI DATI PERSONALI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del GDPR); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva (*“tra le altre, se del caso”*).

Per lo stesso motivo, secondo il GDPR non potranno sussistere obblighi generalizzati di adozione di misure *“minime”* di sicurezza poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del

GDPR.

Per le modalità organizzative con le quali questa SCUOLA ha stabilito di ottemperare all'adempimento sin qui descritto, vale la scelta di fornitori di soluzioni software tra le più diffuse e collaudate in ambito scolastico e di società di gestione della infrastruttura di rete informatica e degli accessi.

NOTIFICA DI UNA VIOLAZIONE DEI DATI PERSONALI ALL'AUTORITA' DI CONTROLLO

Il Titolare deve **notificare all'Autorità di controllo le violazioni di dati personali** di cui vengano a conoscenza, entro 72 ore e comunque *“senza ingiustificato ritardo”*, ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati (si veda considerando 85 del GDPR); questa procedura va sotto il nome di **“Data Breach”**.

Pertanto, la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati che spetta, ancora una volta, al Titolare. Se ciò accade, si dovrà informare della violazione anche gli interessati, sempre *“senza ingiustificato ritardo”*; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del GDPR. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del GDPR.

Il Titolare del trattamento, sentito il DPO, adotta quindi le misure necessarie a documentare eventuali violazioni, essendo peraltro tenuto a fornire tale documentazione, su richiesta, al Garante in caso di accertamenti.

Si ricorda, inoltre, che l'Autorità ha messo a disposizione un modello per la notifica dei trattamenti da parte dei fornitori di servizi di comunicazione elettronica accessibili al pubblico (<http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1915835>) che intende rielaborare al fine di renderlo utilizzabile da tutti i titolari di trattamento secondo quanto prevede il regolamento.

Il predetto modello è allegato al presente Regolamento Applicativo.

VALUTAZIONE DI IMPATTO (VIP) SULLA PROTEZIONE DEI DATI

Le misure di sicurezza devono **“garantire un livello di sicurezza adeguato al rischio”** del trattamento (articolo 32, paragrafo 1 del GDPR); in questo senso, la lista di cui al paragrafo 1 dell'art. 32 è una lista aperta e non esaustiva.

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel GDPR rispetto alla gestione degli obblighi dei titolari, ossia il **rischio inerente al trattamento**.

Quest'ultimo è da intendersi come rischio di impatti negativi sulle libertà e i diritti degli interessati (si vedano considerando 75-77); tali impatti dovranno essere analizzati attraverso un apposito **processo di valutazione** (si vedano artt. 35-36) tenendo conto dei rischi noti o evidenziabili e delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

All'esito di questa valutazione di impatto il Titolare potrà decidere in autonomia se iniziare il trattamento (avendo adottato le misure idonee a mitigare sufficientemente il rischio) ovvero consultare l'autorità di controllo competente per ottenere indicazioni su come gestire il rischio residuale; l'Autorità non avrà il compito di "autorizzare" il trattamento, bensì di indicare le misure ulteriori eventualmente da implementare a cura del titolare e potrà, ove necessario, adottare tutte le misure correttive ai sensi dell'articolo 58: dall'ammonimento del titolare fino alla limitazione o al divieto di procedere al trattamento.

TRASFERIMENTO DI DATI PERSONALI ALL'ESTERO

Si fa rinvio ai principi dettati dal GDPR agli articoli 44 e seguenti, nonché alle indicazioni che fossero dettate, in materia, dal Legislatore nazionale e dal Garante per la protezione dei dati personali.

DISCIPLINA SULLA VIDEOSORVEGLIANZA

Si fa rinvio alle disposizioni di cui al *Regolamento* tempo per tempo vigente, che disciplina la materia di cui si tratta.

DISCIPLINA SULL'UTILIZZO DEI MEZZI INFORMATICI E TELEMATICI

Si fa rinvio alle disposizioni di cui al *Regolamento* tempo per tempo vigente, che disciplina la materia di cui si tratta.

PARTE SESTA ATTUAZIONE IN AMBITO SCOLASTICO DEGLI ADEMPIMENTI EUROPEI

AMBITI DI ATTIVITA' CORRELATI AI NUOVI OBBLIGHI EUROPEI

Gestione della comunicazione interna ed esterna

La comunicazione interna ed esterna è di pertinenza della Presidenza ed è autorizzata dal Dirigente Scolastico dopo attenta valutazione dei contenuti.

Utilizzo di strumenti informatici

Per la gestione degli strumenti informatici si rimanda all'apposito regolamento allegato al presente

Gestione dei social

Trasmissione dei dati personali ai Consigli di classe ai fini della personalizzazione delle attività didattiche

Qualora i consigli di classe abbiano la necessità di visionare dati sensibili legati ad eventuali piani didattici personalizzati gli stessi possono essere visualizzati tramite gli appositi strumenti informatici in dotazione all'Istituto. Gli stessi, dopo l'utilizzo, a cura dei componenti del Consiglio di classe devono essere distrutti in modo sicuro.

Utilizzo dei loghi e dell'immagine dell'Istituzione Scolastica

Video riprese e fotografie interne all'Istituto

Le riprese all'interno dei locali scolastici devono essere autorizzate e la loro riproduzione è soggetta al controllo dei contenuti.

Utilizzo di dati personali al di fuori degli strumenti approvati dal Liceo Michelangiolo

È espressamente vietata la conservazione di copie di dati sensibili al di fuori degli strumenti forniti dall'Istituto (ad esempio su chiavette, copie nelle scrivanie, su pc personali).

Ingresso nelle classi di personale esterno

L'ingresso nelle classi di personale non autorizzato è severamente vietato senza l'autorizzazione del Dirigente.

Qualora l'ingresso sia dovuto a motivi non di emergenza legati alla salute dello studente (supporto, controlli, verifica in loco, etc.) occorre che la richiesta sia approvata dal consiglio di classe e che tutti i genitori della classe sottoscrivano il consenso alla Privacy.

ENTRATA IN VIGORE E PUBBLICITA'

Il presente Regolamento entrerà in vigore dalla data di adozione con atto deliberativo del Consiglio di Istituto.

Il Regolamento verrà pubblicato sul sito internet nell'apposita sezione "privacy".

DISPOSIZIONE FINALE RELATIVA AGLI 'ALLEGATI TECNICI'

Il testo del presente Regolamento potrà essere aggiornato con atto deliberativo del Dirigente Scolastico, su indicazioni del DPO, a seguito di eventuali modifiche che intervengano rispetto alla vigente normativa, sia nazionale che regionale, in materia di protezione dei dati personali.

Gli eventuali aggiornamenti ai *documenti allegati* verranno, pertanto, inseriti in tempo reale sul sito internet nell'apposita sezione dedicata alla "privacy", prescindendo dall'adozione di appositi atti deliberativi di modifica del presente Regolamento e dandone pubblicità per mezzo della mail, così da consentire una rapida consultazione on line dei medesimi e un contenuto sempre aggiornato degli stessi.