

	<b>ISTITUTO COMPRENSIVO CESARE CANTÙ</b> Via Dei Braschi 12 Milano ☎ 0288448318 026468664 Cf 80124430150 – Codice mecc. MIIC8CF006 Pec: <a href="mailto:miic8cf006@pec.istruzione.it">miic8cf006@pec.istruzione.it</a> ; <a href="http://www.icscantu.gov.it">www.icscantu.gov.it</a>	 
Scuola dell'Infanzia Scuola Primaria Scuola Secondaria I grado	Via Dora Baltea 24 tel 0288446937 Cesare Cantù – via Dei Braschi 12 tel 0288448318 Anna Frank – via Dora Baltea 16 tel 0288448371 Umberto Saba – via Del Volga 3 tel 0288447211 fax 0266204676	

Circolare n. 26

Milano, 17/10/2019

A tutto il Personale della Scuola  
Loro SEDI  
Ai Genitori degli Alunni  
Albo –Atti  
Sito Web

**OGGETTO: REGOLAMENTO INTERNO SULLA PROTEZIONE DEI DATI**

Si comunica a tutto il personale dell'ISTITUTO COMPRENSIVO "C. CANTÙ", ai genitori degli alunni frequentanti l'I.C., che dal giorno 21/10/2019 entrerà in vigore il **REGOLAMENTO INTERNO SULLA PROTEZIONE DEI DATI** (approvato con Delibera del Consiglio di Istituto Nr. 15 del 10/10/2019)

Si invitano quanti in indirizzo a prendere visione della normativa e delle relative procedure pubblicate all'albo e sul sito internet della scuola.

IL DIRIGENTE SCOLASTICO  
Prof.ssa Maria Francesca Amendola

*Maria Francesca Amendola*



	<b>ISTITUTO COMPRESIVO CESARE CANTÙ</b> Via Dei Braschi 12 Milano ☎ 0288448318 026468664 Cf 80124430150 – Codice mecc. MIIC8CF006 Pec: <a href="mailto:miic8cf006@pec.istruzione.it">miic8cf006@pec.istruzione.it</a> ; <a href="http://www.icscantu.gov.it">www.icscantu.gov.it</a>	  FONDI STRUTTURALI EUROPEI <b>pon</b> 2014-2020 <small>Programma Operativo Nazionale "Infrastrutture e Trasporti"</small>
Scuola dell'Infanzia Scuola Primaria  Scuola Secondaria I grado	Via Dora Baltea 24 tel 0288446937 Cesare Cantù – Via Dei Braschi 12 tel 0288448318 Anna Frank – Via Dora Baltea 16 tel 0288448371 Umberto Saba – Via Del Volga 3 tel 0288447211 fax 0266204676	

PROT. N. 1212

MILANO17/10/2019

## REGOLAMENTO INTERNO SULLA PROTEZIONE DEI DATI

### PREMESSA DI CARATTERE NORMATIVO

Il presente Regolamento interno in materia di protezione dei dati personali (cosiddetta "privacy") è uno strumento di applicazione del Regolamento Europeo n. 2016/679 o "GDPR", nell'ambito dell'organizzazione dell'Istituto Comprensivo Statale C. Cantù Milano.

A far data dal 25 maggio 2018 trova diretta applicazione, sul territorio nazionale, l'anzidetto Regolamento Europeo sulla privacy, approvato il 27 aprile 2016 e pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016.

Il Regolamento 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. La sua entrata in vigore è stabilita il 24 maggio 2016: entro due anni a partire da tale data, e quindi entro la data del 25 maggio 2018, tutti gli Stati membri dell'Unione dovevano uniformarsi alle nuove regole comunitarie, evitando così di incorrere nelle pesanti sanzioni (sia economiche sia di natura penale) previste dalla nuova normativa.

La data del 25 maggio 2018 è inderogabile, in quanto le prescrizioni stabilite dal Regolamento di cui si tratta trovano diretta ed immediata applicazione, indipendentemente dalla preesistenza di differenti norme nazionali in materia che, quindi, sono automaticamente superate dai precetti del Regolamento n. 2016/679.

Ciò comporta che le disposizioni legislative di cui ex Codice della privacy (D.lgs. 196/2003 e ss.mm.ii.), così come le norme regolamentari emanate negli anni dall'Autorità Garante per la protezione dei dati personali, siano superate, a far data dal 25.05.2018, da quelle del Regolamento UE, nella misura in cui le norme nazionali siano contrastanti o incompatibili con quelle europee e vengono integrate dal Decreto legislativo 10 agosto 2018, n. 101 che adegua il Codice in materia di protezione dei dati personali (Decreto legislativo 30 giugno 2003, n. 196) alle disposizioni del Regolamento (UE) 2016/679 – GDPR.

Il presente Regolamento si rende inoltre necessario per recepire, in un unico testo, i precetti normativi a maggior rilevanza, sia di carattere aziendale che nazionale in tema di trattamento dei dati personali (D.lgs. 196 del 30/06/2003, regolamenti e codici deontologici succeduti negli ultimi anni, direttive e linee guida del Garante, Direttiva dell'UE 2000/58 sulla riservatezza nelle comunicazioni elettroniche e soprattutto Regolamento UE 2016/679 del Parlamento europeo e del Consiglio del 27/04/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati).

### PREMESSA DI CARATTERE ORGANIZZATIVO

Dall'esame della materia emerge come sia, ormai, imprescindibile promuovere un cambiamento di mentalità che porti alla piena tutela della privacy, da considerare non solo come un oneroso rispetto di adempimenti burocratici, ma, soprattutto, come una garanzia per il cittadino-utente che si rivolge alla struttura scolastica, di una completa riservatezza sotto il profilo sostanziale, considerando il diritto alla privacy un diritto inviolabile dell'essere umano che rientra nelle libertà fondamentali del singolo individuo.



La "cultura della privacy" necessita di divenire elemento cardine dell'organizzazione anche della SCUOLA, che deve impegnarsi perché essa possa crescere e rafforzarsi, principalmente fra gli operatori, in quanto solo con la conoscenza minima dei principi fondamentali che stanno alla base della vigente normativa potranno essere adottati correttamente tutti gli adempimenti di carattere tecnico ed organizzativo, nel trattamento dei dati di competenza, con la consapevolezza di contribuire concretamente al miglioramento della qualità del rapporto con l'utenza.

Ai sensi del Nuovo Regolamento Europeo sulla Privacy entrato in vigore il 25 maggio 2018 (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](http://www.garanteprivacy.it) oppure tramite la mail [protocollo@pec.gdpd.it](mailto:protocollo@pec.gdpd.it).

**Titolare del trattamento:**

**Istituto Comprensivo Statale "Cesare Cantù", Milano**

**Rappresentato dal dirigente scolastico Prof.ssa Maria Francesca Amendola**

**Numero di telefono: 02 88448318**

**Indirizzo email: [dirigente@icscantu.gov.it](mailto:dirigente@icscantu.gov.it)**

**Responsabile Protezione Dati (RPD): (da incaricare)**

.....

## PREMESSA DI CARATTERE METODOLOGICO

Vengono allegati a questo Regolamento una serie di documenti tecnici necessari a dare compiuta attuazione, sia verso l'interno che verso l'esterno, ai dettami della nuova "privacy europea": documenti ai quali viene data massima pubblicità e diffusione, tramite la pubblicazione sullo spazio internet.

Tra questi documenti vi sono, a titolo esemplificativo, il modello di accordo per la nomina del Responsabile esterno del trattamento dei dati personali, il modulo per l'informativa ed il consenso al trattamento dei dati, ed il disciplinare sull'utilizzo dei mezzi informatici e telematici della Scuola.

Il principio cardine introdotto dal nuovo Regolamento UE è quello della "responsabilizzazione" (accountability nell'accezione inglese) che pone in carico al Titolare del trattamento dei dati l'obbligo di attuare politiche adeguate in materia di protezione dei dati, con l'adozione di misure tecniche ed organizzative, anche certificate, che siano concretamente e sempre dimostrabili, oltre che conformi alle disposizioni europee (principio della "conformità" o compliance nell'accezione inglese); vi è quindi l'obbligo di porre in essere comportamenti proattivi, tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento. 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.

## DISPOSIZIONI GENERALI

### OGGETTO DEL REGOLAMENTO

Il presente Regolamento disciplina, all'interno dell'Istituto Comprensivo Statale "Cesare Cantù" di Milano, la tutela delle persone in ordine al trattamento dei dati personali, nel rispetto di quanto previsto in conformità all'emanazione della nuova normativa sovranazionale, il Regolamento UE n. 679 del Parlamento Europeo e del Consiglio del 27/04/2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati.

### FINALITÀ' DEL REGOLAMENTO

La Scuola garantisce che il trattamento dei dati, a tutela delle persone fisiche, si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato con



particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali, a prescindere dalla nazionalità o dalla residenza dell'interessato. Ogni persona, infatti, ha diritto alla protezione dei dati di carattere personale che la riguardano (articolo 8, paragrafo 1, della Carta dei diritti fondamentali dell'Unione Europea.)

## **SENSIBILIZZAZIONE**

La Scuola sostiene e promuove, al suo interno, ogni strumento di sensibilizzazione che possa consolidare il pieno rispetto del diritto alla riservatezza e migliorare la qualità del servizio offerto all'utenza.

Uno degli strumenti essenziali di sensibilizzazione, anche in materia di privacy, è l'attività formativa del personale e l'attività informativa diretta a tutti coloro che hanno rapporti con la Scuola.

Per garantire la conoscenza delle disposizioni introdotte dal nuovo Regolamento europeo, e di conseguenza dal presente nuovo Regolamento, al momento dell'ingresso in servizio sarà fornita, a cura della Segreteria, ad ogni dipendente (oltre che ad ogni collaboratore, consulente, esperto esterno) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto di lavoro (o nella lettera di incarico per i soggetti non dipendenti poc'anzi citati), con la quale detti soggetti (dipendenti e non dipendenti) sono nominati quali "autorizzati al trattamento dei dati" ai sensi del Regolamento UE2016/679.

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

Il Regolamento, pubblicato sul sito, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale.

## **DEFINIZIONI**

Come stabilito dall'articolo n. 4 del Regolamento Europeo n. 2016/679, ai fini di questo disciplinare si intende per:

- 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 o sociale;
- 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 Regolamento Europeo n. 2016/679, 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 Regolamento UE, 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 dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»). Come stabilito dal Regolamento UE, il Titolare del trattamento (Dirigente Scolastico della Scuola) è competente per il rispetto di quanto sin qui esposto ed è in grado di provarlo 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.

Si fa ulteriore 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 Regolamento Europeo n.2016/679, "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."

Si fa ulteriore 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.

## **DIRITTI DELL'INTERESSATO**

### **INFORMATIVA SUL TRATTAMENTO DEI DATI**

Come stabilito dall'articolo n.13 del Regolamento Europeo n.2016/679, 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.

## I DATI

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.

Alla luce dei principi esposti, si rinvia ai documenti presenti nella sezione dedicata alla Privacy del sito della scuola ("Modulistica relativa all'informativa e al consenso al trattamento dei dati").

## CONSENSO AL TRATTAMENTO DEI DATI: PRINCIPI GENERALI

Il Regolamento UE conferma che ogni trattamento deve trovare fondamento in un'ideale base giuridica; i fondamenti di liceità del trattamento sono indicati all'art. 6 del Regolamento e coincidono, in linea di massima, con quelli previsti attualmente dal vigente Codice della privacy (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 dei genitori o di chi ne fa le veci (articolo n. 8 del Regolamento Europeo).



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 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 Regolamento UE).

**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 Regolamento Europeo n.2016/679, 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.

I principi su esposti sono recepiti anche nei documenti presenti nella sezione dedicata alla Privacy del sito della scuola, ove è prodotto sia il modello di "Informativa" che quello di raccolta del "consenso", sia che ciò avvenga nei confronti di persone adulte e capaci, che di soggetti minori ed incapaci.

Per quanto riguarda, inoltre, le modalità concrete per mezzo delle quali trova attuazione, nell'attuale contesto normativo ed 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.

Si fa espresso rinvio, in particolare, alle vigenti disposizioni normative in materia di "accesso documentale", di "accesso civico" e di "accesso generalizzato".

Nel dare evidenza del fatto che, presso questa SCUOLA, la competenza sulla materia de quo è affidata al Responsabile della Trasparenza e della Prevenzione della Corruzione, si rinvia al contenuto delle schede informative pubblicate sul sito internet, dedicate all'argomento.

A tale riguardo, nel rinviare a quanto pubblicato al sito web, si fa presente che:

a) per accesso documentale si intende la domanda di accesso (richiesta di presa visione o di rilascio copia) a delibere e provvedimenti della Scuola, nei termini e alle modalità previste dalla normativa vigente (Legge 07 agosto 1990 n. 241 e ss.mm.ii. e D.P.R. 12 aprile 2006 n. 184).

Possono fare domanda tutti i cittadini portatori di un interesse "diretto, concreto e attuale, Regolamento interno sulla protezione dei dati corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è richiesto l'accesso" (art. 22, Legge 241/1990).

Per presentare domanda, è necessario rivolgersi all'Ufficio che detiene il documento di cui si chiede l'accesso, portando con sé il proprio documento di identità valido. I costi di ricerca, visura e riproduzione fotostatica, e le spese di spedizione, sono quelle previste dal tariffario in vigore.

**Il procedimento di accesso si conclude entro 30 giorni, decorrenti dalla presentazione della richiesta all'ufficio competente (art. 6 del D.P.R. 184 del 2006).**

b) per accesso civico si intende il diritto di chiunque di richiedere documenti, informazioni o dati che le pubbliche amministrazioni non hanno pubblicato pur avendone l'obbligo (Decreto Legislativo 97 del 17/5/2016 "Revisione e semplificazione delle disposizioni in materia di prevenzione della corruzione pubblicità e trasparenza delle Amministrazioni Pubbliche", e Decreto Legislativo 33 del 14/03/2013: "Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni").

La richiesta viene presentata al Responsabile della Prevenzione della Corruzione e della Trasparenza della SCUOLA utilizzando il modulo prodotto sul sito internet. La Scuola, entro 30 giorni, procede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto. Se il documento, l'informazione o il dato richiesti risultano già pubblicati nel rispetto della normativa vigente, la Scuola indica al richiedente il relativo collegamento ipertestuale. Nei casi di ritardo o mancata risposta il richiedente può ricorrere al titolare del potere sostitutivo (indicato sul sito web) che, verificata la sussistenza dell'obbligo di pubblicazione, provvede alla pubblicazione nel sito del documento, dell'informazione o del dato richiesto e lo trasmette contestualmente al richiedente, ovvero comunica al medesimo l'avvenuta pubblicazione, indicando il collegamento ipertestuale a quanto richiesto.



c) per accesso generalizzato si intende il diritto di chiunque di accedere ai dati e ai documenti detenuti dalle Pubbliche Amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione ai sensi del Decreto Legislativo 33/2013 ("Decreto Trasparenza") e del D.lgs. 97/2016 (così detto Freedom of Information Act o "FOIA"), nel rispetto dei limiti relativi alla tutela di interessi giuridicamente rilevanti, allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico.

La richiesta viene presentata:

a) all'Unità che detiene i dati, le informazioni o i documenti;

b) all'Ufficio Relazioni con il Pubblico utilizzando il modulo pubblicato sul sito internet.

Il procedimento di accesso generalizzato deve concludersi con provvedimento espresso e motivato nel termine di 30 giorni dalla presentazione dell'istanza, con la comunicazione dell'esito al richiedente e agli eventuali controinteressati. Tali termini sono sospesi (fino ad un massimo di 10 giorni) nel caso di comunicazione della richiesta al controinteressato. Se il documento risulta già pubblicato nel sito nel rispetto della normativa vigente, la Scuola indica al richiedente il relativo collegamento ipertestuale.

Nei casi di diniego totale o parziale dell'accesso o di mancata risposta entro il termine indicato, il richiedente può presentare richiesta di riesame al Responsabile della Prevenzione della Corruzione e della Trasparenza, che decide con provvedimento motivato, entro il termine di 20 giorni. Se l'accesso è stato negato o differito il suddetto Responsabile provvede sentito il Garante per la protezione dei dati personali, il quale si pronuncia entro il termine di 10 giorni dalla richiesta. A decorrere dalla comunicazione al Garante, il termine per l'adozione del provvedimento da parte del Responsabile è sospeso fino alla ricezione del parere del Garante e comunque per un periodo non superiore ai predetti 10 giorni. Avverso la decisione dell'amministrazione competente o, in caso di richiesta di riesame, avverso quella del Responsabile della Prevenzione della Corruzione e della Trasparenza, il richiedente può proporre ricorso al tribunale amministrativo regionale (TAR).

#### **DIRITTO DI RETTIFICA**

Come stabilito dall'articolo n.16 del Regolamento Europeo n.2016/679, 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 Regolamento Europeo n.2016/679, 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 Regolamento UE).

Ha un campo di applicazione più esteso di quello di cui all'art. 7, comma 3, lettera b), del Codice della privacy, poiché l'interessato ha il diritto di chiedere la cancellazione dei propri dati personali, per esempio, che dopo revoca del consenso al trattamento.

#### **DIRITTO DI LIMITAZIONE AL TRATTAMENTO**

Si tratta di un diritto diverso e più esteso rispetto al "blocco" del trattamento di cui all'art. 7, comma 3, lettera a), del Codice: in particolare, 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 per altri trattamenti 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 Regolamento UE). 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 Regolamento Europeo n.2016/679, 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 Regolamento Europeo n.2016/679, 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.

## **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 della Scuola stessa, con sede in Via Dei Braschi 12.

Il Titolare, avvalendosi della supervisione e collaborazione del Data Protection Officer 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) a 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) a nominare il Data Protection Officer, come stabilito dall'articolo 37 del Regolamento UE;

d) a disporre periodiche verifiche sul rispetto delle istruzioni impartite, anche con riguardo agli aspetti relativi alla sicurezza dei dati;

e) a 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 Regolamento UE 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 Regolamento).

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.

## **CONTITOLARI DEL TRATTAMENTO**

Come stabilito dall'articolo n. 26 del Regolamento Europeo n. 2016/679, 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 Regolamento UE nei confronti di e contro ciascun Titolare del trattamento.

## **RESPONSABILE INTERNO DEL TRATTAMENTO DEI DATI**

Secondo il codice europeo 679/2016, s'intende per Responsabile del trattamento dei dati, "la persona fisica, giuridica, la Pubblica Amministrazione e qualsiasi altro Ente, Associazione ed Organismo preposti dal Titolare al trattamento di dati personali". La SCUOLA può designare i Responsabili interni del trattamento dei dati personali, conferendo l'incarico a quei dipendenti che presentino garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate a far sì che il trattamento soddisfi i requisiti del presente Regolamento e garantisca la tutela dei diritti dell'interessato.

**Nell'ambito della SCUOLA, vengono quindi individuati quali Responsabili interni del trattamento dei dati personali:**

- per la presidenza la docente : Ornaghi Sabrina**
- per la funzione di segreteria : Dsga Serra Salvatore**
- per le attività delle funzioni strumentali i docenti Di Bartolomeo Cristina, Molon Maddalena, Bertasi Marco , Cozzi Albino, Caimi Elena**
- per le attività di orientamento : Funzioni strumentali Battigaglia Elena, Cirillo Antonella, Battaglia Sandro**
- per le attività di gestione informatica i docenti Perrera Daniela, Mauri Enrico**

Il Titolare del trattamento dei dati deve informare ciascun Responsabile del trattamento dei dati, così come individuato dal presente Regolamento, delle responsabilità che gli sono affidate in relazione a quanto disposto dalle normative vigenti. I responsabili del



trattamento rispondono al Titolare di ogni violazione o mancata attivazione di quanto dettato dalla normativa vigente.

Il Responsabile interno del trattamento 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.

Il Responsabile per il trattamento dei dati personali, nell'espletamento della sua funzione, deve inoltre collaborare con il Data Protection Officer (DPO), al fine di: a) comunicare al DPO, quando questi ne faccia richiesta, ogni notizia rilevante ai fini dell'osservanza degli obblighi dettati dagli articoli da 32 a 36 del Regolamento UE 2016/679 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.

- b) utilizzare il modello di Informativa e Consenso allegato al presente Regolamento, verificandone il rispetto e fornendo al DPO, quando questi ne faccia richiesta, le informazioni utili per l'aggiornamento del registro dei trattamenti;
- c) rispondere alle istanze degli interessati secondo quanto stabilito dal Codice della privacy e stabilire modalità organizzative volte a facilitare l'esercizio del diritto di accesso dell'interessato e la valutazione del bilanciamento degli interessi in gioco;
- d) contribuire a far sì che tutte le misure di sicurezza riguardanti i dati della Scuola siano applicate all'interno della Scuola stessa ed all'esterno, qualora agli stessi vi sia accesso da parte di soggetti terzi quali Responsabili del trattamento;
- e) informare il Titolare del trattamento, senza ingiustificato ritardo, della conoscenza dell'avvenuta violazione dei dati personali.

Questa SCUOLA provvederà alla nomina dei Responsabili interni del trattamento dei dati, dandone comunicazione personale a ciascun Responsabile all'uopo nominato.

#### **RESPONSABILE ESTERNO DEL TRATTAMENTO DEI DATI**

Nell'ambito della SCUOLA, sono inoltre individuati quali Responsabili "esterni" del trattamento dei dati personali, tutti i soggetti esterni che, per svolgere la propria attività sulla base di una convenzione o un contratto sottoscritto con la SCUOLA, trattino dati di cui è titolare la SCUOLA medesima e qualora siano in possesso dei requisiti previsti dall'articolo 29, primo comma, del Codice della privacy (esperienza, capacità ed affidabilità). In ottemperanza al nuovo articolo 28 del Regolamento Europeo 2016/679, i Responsabili esterni 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, dei pazienti (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 Regolamento Europeo 2016/679 rubricato "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 un "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.

Dopo l'approvazione del presente Regolamento, si provvederà a trasmettere il presente Regolamento a tutte le strutture interessate, evidenziando la necessità di provvedere alle nomine dei Responsabili esterni utilizzando la nuova modulistica prevista.

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 Regolamento Europeo si sofferma sul fatto che chi tratta dati, ricevendo istruzioni e formazione da parte del Titolare del trattamento debba da questi essere "autorizzato al trattamento" (articoli 4 e 10 del Regolamento).

Come già stabilito all'articolo 6 del presente Regolamento, al momento dell'ingresso in servizio è fornita, ad ogni dipendente (oltre che ad ogni collaboratore, consulente) una specifica comunicazione in materia di privacy, con apposita clausola inserita nel contratto



di lavoro (o nella lettera di incarico per i summenzionati soggetti non dipendenti), con la quale detti soggetti(dipendenti e non dipendenti) vengono nominati quali "autorizzati al trattamento dei dati" ai sensi del Regolamento UE 2016/679.

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

Il Regolamento, pubblicato sul sito, contiene infatti tutti i principi fondamentali della materia, esposti in maniera semplice, chiara e puntuale e il dipendente (o il non dipendente nei termini di cui si è detto sopra),nel sottoscrivere il contratto di lavoro (o la lettera di incarico), è reso edotto dell'esistenza dell'anzidetto Regolamento e delle modalità di consultazione del medesimo. Analoghe considerazioni valgono per la figura autorizzato esterno: tutti coloro che svolgono un'attività di trattamento dei dati nell'ambito di questa SCUOLA, pur non essendo dipendenti e neppure titolari di incarichi conferiti dalla medesima (quali consulenze, collaborazioni o borse di studio conferite dalla SCUOLA), devono essere designati da parte del Responsabile (in questo caso "esterno")tramite una lettera (o una nota) di nomina come autorizzati esterni.Ci si riferisce, a titolo esemplificativo, al personale tirocinante o al personale volontario che opera contemporaneamente 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 RDP è obbligatoria in tutte le organizzazioni, anche pubbliche, che trattano come attività principali i dati sensibili su larga scala,come ospedali,assicurazioni e istituti di credito. Chi svolge la funzione di RPD, quindi, deve presentare caratteristiche di indipendenza ed autorevolezza, oltre che competenze manageriali. Non deve, inoltre, essere in conflitto di interessi in quanto il Regolamento UE vieta di nominare RDP anche chi, solo in astratto, possa potenzialmente trovarsi in conflitto di interessi. Si tratta di una figura dirigenziale, di alta professionalità, a metà tra il consulente ed il revisore e non dovrebbe ricoprire ruoli gestionali rispetto all'attività della Scuola o ai fini istituzionali della Pubblica Amministrazione.

Ai sensi dell'articolo 39 del Regolamento UE, 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 ditrattamento.

Ai sensi dell'articolo 37 del Regolamento UE, Egli 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 (RPD esterno);

4. disporre di risorse umane e finanziarie, messe a disposizione dal Titolare, per adempiere ai suoi scopi.

Il Regolamento UE prevede la pubblicazione on line del curriculum del RPD, nonché la pubblicazione sul sito istituzionale dell'Ente dei "dati di contatto" del RPD: dati che debbono essere inseriti anche nell'informativa sul trattamento dei dati, così che il RPD sia agevolmente contattabile dai cittadini-utenti ma anche dal Garante per la privacy.

### **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 Regolamento Europeo n. 2016/679 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 Regolamento UE) 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 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 Regolamento UE); 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 Regolamento UE non potranno sussistere obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art. 33 Codice) poiché tale valutazione sarà rimessa, caso per caso, al titolare e al responsabile in rapporto ai rischi specificamente individuati come da art. 32 del regolamento.

Tuttavia, facendo anche riferimento alle prescrizioni contenute, in particolare, nell'Allegato "B" al Codice, l'Autorità potrà valutare la definizione di linee-guida o buone prassi sulla base dei risultati positivi conseguiti in questi anni; inoltre, per alcune tipologie di trattamenti (quelli di cui all'art. 6, paragrafo 1, lettere c) ed e) del regolamento) potranno restare in vigore (in base all'art. 6, paragrafo 2, del regolamento) le misure di sicurezza attualmente previste attraverso le disposizioni di legge volta per volta applicabili: è il caso, in particolare, dei trattamenti di dati sensibili svolti dai soggetti pubblici per finalità di rilevante interesse pubblico nel rispetto degli specifici regolamenti attuativi (ex artt. 20 e 22 Codice), ove questi ultimi contengano disposizioni in materia di sicurezza dei trattamenti.

Per le modalità organizzative con le quali questa SCUOLA ha stabilito di ottemperare all'adempimento sin qui descritto, vale il presente regolamento e l'obbligo di predisporre le più idonee misure di sicurezza a livello informatico, adeguando le misure minime e valutandone gli impatti, anche curando l'aggiornamento (e/o la riedizione) del Documento Programmatico sulla Sicurezza (D.P.S.).



## **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 Regolamento UE); 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 la probabilità di tale rischio è elevata, si dovrà informare della violazione anche gli interessati, sempre "senza ingiustificato ritardo"; fanno eccezione le circostanze indicate al paragrafo 3 dell'articolo 34 del Regolamento UE, che coincidono solo in parte con quelle attualmente menzionate nell'art. 32-bis del Codice. I contenuti della notifica all'Autorità e della comunicazione agli interessati sono indicati, in via non esclusiva, agli art. 33 e 34 del regolamento. Il Titolare del trattamento, sentito il Data Protection Officer, 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/-/docwebdisplay/docweb/1915835>)

## **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 Regolamento UE); 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").

Fondamentali fra tali attività correlate alla sicurezza sono quelle connesse al secondo criterio individuato nel Regolamento UE 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 Regolamento Europeo 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.



