Il nuovo Regolamento UE in materia di protezione dei dati personali

Regolamento (UE) 2016/679 del Parlamento europeo e Del Consiglio del 27 aprile 2016

Facciamo chiarezza

Cosa fare

Cosa cambia

Cosa non cambia

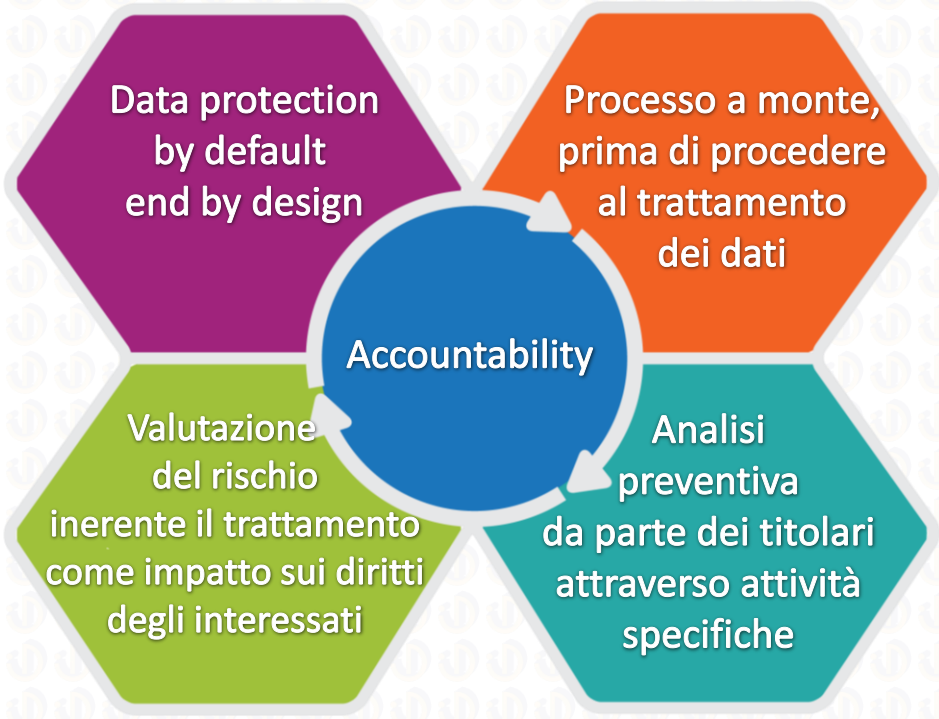
Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

Le cose da fare nell' imminenza sono :

- **Nomina RPD/DPO**
- **Adeguamento Informativa**
- **Predisposizione Registro dei trattamenti**

in conformità al principio di "responsabilizzazione" (accountability) (artt.23-25), a partire dal criterio "data protection by default and by design" (art.25).

E' la 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.



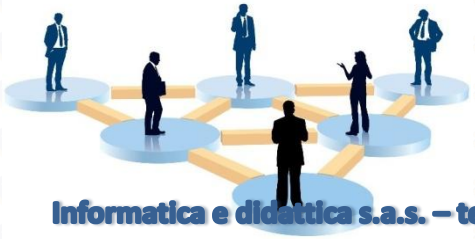
Ruoli nella scuola

Il **Titolare del trattamento** è chi determina il motivo e le modalità del trattamento, ed è responsabile giuridicamente dell'ottemperanza degli obblighi previsti dalla normativa: la scuola è il titolare del trattamento nella persona del legale rappresentante, il **Dirigente scolastico.**

Il **responsabile del trattamento** è la persona fisica, giuridica, pubblica amministrazione o ente che tratta i dati personali per conto del titolare del trattamento. Nella scuola si individua il *responsabile (solo esterno)* quando ricorrano i presupposti: es. fornitore che tratta dati per conto della scuola (Axios, Argo, ecc. che trattano i dati della scuola in cloud), sulla base di un contratto o altro atto giuridico che vincoli il responsabile del trattamento al titolare.

Il **RPD** è la figura che assume il ruolo di supervisore indipendente, che fornisce consulenza al titolare e al responsabile sugli obblighi previsti dal GDPR, controlla l'osservanza del Regolamento e l'assegnazione dei ruoli all'interno dell'Ente: è soggetto esterno nominato dal titolare.

L' **incaricato** è la persona fisica incaricata dal titolare o dal responsabile a compiere operazioni di trattamento dati: nella scuola sono i dipendenti.



L' **interessato** è la persona fisica a cui si riferiscono i dati personali, o più esattamente il proprietario dei suoi dati: nella scuola sono gli alunni, il personale, i familiari e tutti i soggetti dei quali si posseggono e trattano i dati.

Iniziamo da "COSA FARE"
Le priorità per le PA

Partiamo dal principio fondamentale introdotto dal Regolamento, il principio di "responsabilizzazione" (accountability), che attribuisce direttamente ai titolari del trattamento il compito di assicurare, ed essere in grado di comprovare, il rispetto dei principi applicabili al trattamento dei dati personali (art.5)

1. Nomina del Responsabile della protezione dei dati – RPD/DPO (artt.37-39) obbligatoria per le PA

- Tra il personale dipendente in organico (dove possibile)
- Tramite affidamento all'esterno, in base a un contratto di servizi

Il DPO (o RPD) deve:

- conoscere la normativa di riferimento
- conoscere lo specifico settore di attività e la struttura organizzativa del titolare (scuola)
- conoscere le operazioni di trattamento dati effettuate dal titolare (scuola) e le tecnologie informatiche utilizzate
- contribuire a dare attuazione agli elementi essenziali del regolamento (incarichi, diritti degli interessati, registri delle attività …)
- consigliare il titolare e i dipendenti in merito agli obblighi e verificare l'applicazione della normativa
- fornire, se richiesto, un parere in merito alla valutazione d'impatto sulla protezione dei dati
- ricevere le risorse finanziarie, infrastrutturali e umane necessarie per assolvere ai compiti previsti

Più organismi pubblici possono nominare → Un unico DPO (RPD) Art. 37 par. 3

Il Titolare deve individuare una figura:

Che abbia esperienza nella gestione della materia di riferimento e conosca le procedure che caratterizzano il settore in cui operare (in questo caso la scuola)

Di cui si fidi

E' comunque il titolare del trattamento a dover garantire e dimostrare la conformità al GDPR rispondendo pertanto in via esclusiva anche ad eventuali sanzioni amministrative.

2. Adeguare l'Informativa alle nuove disposizioni del Regolamento

E' opportuno che i titolari del trattamento verifichino la rispondenza delle informative attualmente utilizzate a tutti i criteri previsti dal Regolamento UE, con particolare riguardo ai contenuti obbligatori e alle modalità di redazione, in modo da apportare le modifiche/integrazioni necessarie entro il 25 maggio 2018.

3. Predisporre il Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento [...] (art.30), devono tenere un registro dei trattamenti: si tratta di uno strumento fondamentale non solo in caso di un'eventuale supervisione del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un'azienda o soggetto pubblico, indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta del Garante.
I contenuti del registro sono fissati nell'art.30, ma il titolare può inserire ulteriori informazioni se lo riterrà opportuno.

Come fare?
Se vorrete … ci penseremo noi!

In continuità con il lavoro svolto durante questi anni (a partire dal D.lgs 196/2003) con tantissime scuole, ad oggi tutte in regola con gli adempimenti privacy previsti dal Codice, Informatica e Didattica s.a.s. si propone come supporto alla scuola in questa transizione verso il nuovo Regolamento UE, mettendo in attuazione gli adempimenti previsti.

In relazione a quanto previsto, proponiamo la nomina di RPD (Responsabile per la Protezione dei Dati) a nostro nome, così da:

- Valutare lo stato degli adempimenti posti in essere dalla scuola (chi è allineato all'attuale normativa ha già un bel vantaggio) e adeguare o riorganizzare completamente in base a quanto previsto dal nuovo Regolamento
- Supportare e non solo "consigliare", a partire dai primi adempimenti (adeguamento Informativa e predisposizione Registro dei trattamenti) e a seguire con tutti gli altri che dovranno essere predisposti
- Contenere i costi

Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

COSA CAMBIA – COSA NON CAMBIA

Regolamento UE 2016/679

Principali novità
e approcci operativi

- Titolare, responsabile, incaricato
- Accountability e rischio
- Fondamenti di liceità del trattamento
- Informativa
- Diritti degli interessati

Titolare, responsabile, incarico del trattamento

COSA CAMBIA

Il Regolamento:

• disciplina la contitolarità del trattamento (art.26) e impone ai titolari di definire specificamente (con un atto giuridicamente valido) il rispettivo ambito di responsabilità e i compiti con particolare riguardo all'esercizio dei diritti degli interessati, che hanno la possibilità di rivolgersi indifferentemente a uno qualsiasi dei titolari operanti congiuntamente;

• fissa più dettagliatamente le caratteristiche dell'atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi di un atto giuridico e deve disciplinare tassativamente almeno le materie riportate al paragrafo 3 dell'art.28;

• consente la nomina di sub-responsabili del trattamento da parte di un responsabile, per specifiche attività di trattamento, nel rispetto degli stessi obblighi che legano il titolare al responsabile primario; quest'ultimo risponde dinanzi al titolare dell'inadempimento del sub-responsabile, salvo dimostri che un eventuale evento dannoso "non gli è in alcun modo imputabile".

COSA CAMBIA

- Prevede obblighi specifici in capo ai responsabili del trattamento; in particolare, ciò riguarda:
  – L a tenuta del registro dei trattamenti svolti (art.30)
  – L'adozione di idonee misure tecniche e organizzative per garantire la sicurezza dei trattamenti
  – La designazione di un RPD/DPO, nei casi previsti

COSA NON CAMBIA

Il Regolamento definisce caratteristiche soggettive e responsabilità di titolare e responsabile del trattamento negli stessi termini del Codice italiano. Pur non prevedendo espressamente la figura dell' "incaricato" del trattamento (ex art.30 del Codice), il Regolamento non ne esclude la presenza in quanto fa riferimento a "persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile".

Alla luce del principio di "responsabilizzazione", è opportuno che i titolari mantengano in essere la struttura organizzativa e le modalità di designazione degli incaricati di trattamento così come delineatesi in virtù del Codice.

Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

Misure di Accountability

COSA CAMBIA

Il regolamento pone l'accento sulla "responsabilizzazione" (accountability) del titolare, cioè sull'adozione di comportamenti proattivi e tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del Regolamento (artt.23-25).
Si affida così ai titolari il compito di decidere autonomamente le modalità, le garanzie e i limiti del trattamento dei dati personali, nel rispetto delle disposizioni normative.

Primo criterio:
"data protection by default end by design" (art.25)

Prevedere 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. Ciò deve avvenire a monte, prima di procedere al trattamento, e richiede un'analisi preventiva da parte dei titolari che deve concretizzarsi in una serie di attività specifiche e dimostrabili.

Secondo criterio:
"rischio inerente il trattamento"

E' il rischio di impatti negativi sulle libertà e i diritti degli interessati, che dovranno essere analizzati attraverso un apposito processo di valutazione (artt.35-36), andando ad individuare le misure tecniche e organizzative per mitigare tali rischi. All'esito di tale valutazione, il titolare deciderà se iniziare il trattamento o consultare l'autorità di competente per ottenere indicazioni.

Adempimenti da parte dei titolari del trattamento

Registro dei trattamenti

COSA CAMBIA

Tutti i titolari di trattamento [...] devono tenere un registro delle operazioni di trattamento i cui contenuti sono indicati all'art.30.
E' uno strumento FONDAMENTALE non solo per la eventuale supervisione da parte del Garante, ma anche per disporre di un quadro aggiornato dei trattamenti effettuati ai fini della valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica.
Non è un adempimento formale ma parte integrante di un sistema di corretta gestione dei dati personali.

Misure di sicurezza

COSA CAMBIA

Le misure di sicurezza devono "garantire un livello di sicurezza adeguato al rischio" (art.32); in questo senso, la lista di cui all. art.32 è una lista aperta e non esaustiva. Dopo il 25 maggio 2018, non esisteranno obblighi generalizzati di adozione di misure "minime" di sicurezza (ex art.33 Codice) ma tale valutazione sarà rimessa al titolare in rapporto ai rischi individuati. Tuttavia l'Autorità (facendo anche riferimento all'Allegato B del Codice), potrà valutare la definizione di linee-guida o buone prassi sulla base di quanto fatto in questi anni. Per alcune tipologie di trattamenti (art.6, par.1, lett. C) ed e)) potranno restare in vigore le misure di sicurezza attualmente previste.

Misure di Accountability

Adempimenti da parte dei titolari del trattamento

Notifica delle violazioni di dati personali

COSA CAMBIA

A partire dal 25 maggio 2018, tutti i titolari, dovranno notificare all'Autorità di controllo le violazioni di dati personali di cui vengano a conoscenza, entro 72 ore e comunque "senza giustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.
Tutti i titolari dovranno in ogni caso documentare le violazioni di dati personali subite, anche se non notificate all'autorità di controllo e non comunicate agli interessati, nonché le relative circostanze.

Responsabile della protezione dei dati

COSA CAMBIA

La nomina del RPD/DPO è finalizzata a facilitare l'attuazione del Regolamento da parte del titolare. Infatti, tra i compiti del RPD rientrano "la sensibilizzazione e la formazione del personale" e la sorveglianza sul rispetto degli adempimenti. La sua designazione è obbligatoria in alcuni casi (art.37) e le caratteristiche principali sono:
indipendenza – qualità professionali - conoscenza del settore in cui va ad operare e dei sistemi organizzativi e strumentali.

Misure di Accountability

Fondamenti di liceità del trattamento

I fondamenti di liceità del trattamento (**art. 6 del Regolamento**) coincidono sostanzialmente con quelli previsti dall'attuale Codice privacy (D.lgs 196/2003): 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.

CONSENSO

COSA CAMBIA

- Per i dati "sensibili" (art. 9) e i trattamenti automatizzati (art. 22) il consenso DEVE essere "esplicito".
- NON deve essere necessariamente scritto ma il titolare DEVE essere in grado di dimostrare che l'interessato ha prestato il consenso (la forma scritta, dunque, è comunque idonea a garantire inequivocabilità).
- Il consenso dei MINORI è valido a partire dei 16 anni, prima è necessario il consenso dei genitori o di chi ne fa le veci.

COSA NON CAMBIA

- DEVE essere SEMPRE libero, specifico, informato e inequivocabile; NON è ammesso il consenso tacito o presunto.
- DEVE essere manifestato attraverso "dichiarazione o azione positiva inequivocabile" .

INTERESSE LEGITTIMO PREVALENTE DI UN TITOLARE O DI UN TERZO

COSA CAMBIA

Il BILANCIAMENTO fra legittimo interesse del titolare o del terzo e diritti dell'interessato non spetta all'Autorità ma E' COMPITO DELLO STESSO TITOLARE . E' una delle principali espressioni del principio di "responsabilizzazione" introdotto dal Regolamento.

COSA NON CAMBIA

L'interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell'interessato per costituire fondamento di liceità.

Fondamenti di liceità del trattamento

INFORMATIVA

Contenuti dell'informativa

COSA CAMBIA

• I contenuti dell'informativa sono elencati in MODO TASSATIVO negli artt. 13 e 14 del Regolamento; in particolare, il titolare DEVE SEMPRE specificare i dati di contatto del RPD/DPO, la base giuridica del trattamento, l'eventuale interesse legittimo, se trasferisce dati a Paesi terzi ed, eventualmente, con quali strumenti.

• Ulteriori informazioni necessarie: il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione.

• Se il trattamento prevede processi automatizzati, l'informativa deve specificarlo e indicare la logica e le conseguenze di tali processi.

Tempi dell'informativa

COSA CAMBIA

Nel caso di dati personali non raccolti direttamente presso l'interessato (art.14), l'informativa deve essere fornita entro un termine ragionevole che non può superare 1 mese dalla raccolta, oppure al momento della comunicazione dei dati a terzi (diversamente da quanto previsto dall'art.13 del Codice).

Modalità dell'informativa

COSA CAMBIA

- L'informativa deve avere forma concisa, trasparente, intellegibile per l'interessato e facilmente accessibile; deve essere formulata in un linguaggio chiaro e semplice e per i minori è necessario prevedere informative idonee.

- L'informativa è data, in linea di principio, per iscritto e preferibilmente in formato elettronico, anche se sono ammessi "altri mezzi" (oralmente). Il regolamento ammette l'utilizzo di ICONE per presentare i contenuti dell'informativa in forma sintetica, ma solo "in combinazione" con l'informativa estesa (art.12 par.7); queste icone saranno identica in tutta l'UE e saranno definite prossimamente dalla Commissione europea.

- Sono parzialmente diversi i requisiti che il Regolamento fissa per l'esonero dall'informativa (artt.13, 14 e 23).

COSA NON CAMBIA

L'informativa deve essere fornita all'interessato prima di effettuare la raccolta dei dati (se raccolti direttamente presso l'interessato – art.13 del Regolamento). Se non sono raccolti presso l'interessato (art.14), l'informativa deve comprendere anche le categorie dei dati personali oggetto di trattamento. In tutti i casi, il titolare deve specificare la propria identità, le finalità del trattamento, i diritti degli interessati (compresa la portabilità dei dati), l'eventuale responsabile del trattamento dati e i destinatari dei dati.

Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

Diritti degli interessati

Modalità per l'esercizio dei diritti (artt. 11 e 12)

COSA CAMBIA

- Il termine per la risposta all'interessato è, per tutti i diritti (anche quello di accesso), di 1 mese, estendibile fino a 3 mesi in casi particolari; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

- Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma solo se si tratta di richieste manifestamente infondate o eccessive. Il riscontro all'interessato deve avvenire di regola in forma scritta anche attraverso strumenti elettronici; può essere dato oralmente solo se così richiesto dall'interessato stesso (artt. 12 e 15).

- La risposta fornita all'interessato deve essere concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

Modalità per l'esercizio dei diritti (artt. 11 e 12)

COSA NON CAMBIA

Il titolare del trattamento deve agevolare l'esercizio dei diritti da parte dell'interessato, adottando ogni misura idonea. Il responsabile è tenuto a collaborare con il titolare ai fini dell'esercizio dei diritti degli interessati.

L'esercizio dei diritti è, in linea di principio, gratuito per l'interessato, ma possono esservi delle eccezioni.

Sono ammesse deroghe ai diritti riconosciuti dal Regolamento, ma solo sul fondamento di disposizioni normative nazionali (art.23). In tal senso, possono continuare a essere applicate tutte le deroghe previste dall'art.8 comma 2 del Codice in quanto compatibili.

Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

Diritto di accesso (art.15)

COSA CAMBIA

- Il diritto di accesso prevede in ogni caso il diritto di ricevere una copia dei dati personali oggetto di trattamento.

- Fra le informazioni che il titolare deve fornire non rientrano le "modalità" del trattamento, mentre occorre indicare il periodo di conservazione o i criteri utilizzati per definire tale periodo.

Diritto di cancellazione (diritto all'oblio) (art.17)

COSA CAMBIA

Il diritto all'oblio è il diritto alla cancellazione dei propri dati personali in forma rafforzata. Si prevede, infatti, l'obbligo per i titolari (se hanno reso pubblici i dati ad esempio pubblicandoli sul sito web) di informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi eventuali link.

Diritto di limitazione del trattamento (art.18)

COSA CAMBIA

- E' esercitabile non solo in caso di violazione dei presupposti di liceità del trattamento, ma anche se l'interessato chiede la rettifica dei dati (in attesa di tale rettifica) o si oppone al loro trattamento (art.21)

- Il diritto alla limitazione prevede che il dato personale sia "contrassegnato" in attesa di ulteriori determinazioni; è quindi opportuno che i titolari prevedano nei propri sistemi informativi (elettronici e non) misure idonee a tale scopo.

Diritti degli interessati

Diritto alla portabilità dei dati (art.20)

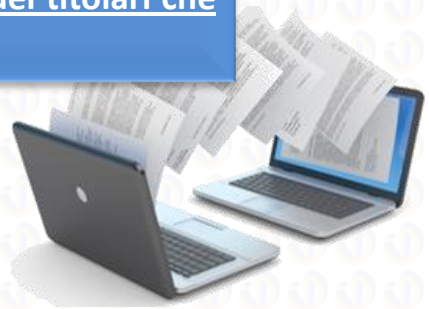
COSA CAMBIA

• 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. Sono portabili solo i dati trattati con il consenso dell'interessato o sulla base di un contratto stipulato con l'interessato e solo i dati che siano stati forniti dall'interessato al titolare (quindi non si applica ai dati il cui trattamento si fonda sull'interesse pubblico o su quello legittimo del titolare).

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

•Poiché la trasmissione dei dati da un titolare a un altro prevede l'utilizzo di formati interoperabili, i titolari che devono applicare tale diritto dovrebbero adottare da subito le misure necessarie a produrre i dati richiesti in un formato interoperabile, secondo le indicazioni fornite al considerando 68 e nelle linee guida del Gruppo "articolo 29".

• Per sua natura, tale diritto non dovrebbe essere esercitato nei confronti dei titolari che trattano dati personali nell'esercizio delle loro funzioni pubbliche.



Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it

CONTESTO NAZIONALE: COSA DEVE FARE IL GOVERNO ITALIANO
DELEGA AL GOVERNO E TEMPI DI ATTUAZIONE

Nell'ambito del disegno di legge per il recepimento delle direttive europee e l'attuazione di altri atti dell'Unione europea (Legge di delegazione europea 2016-2017) è stata prevista la delega al Governo per dare attuazione alla Direttiva (UE) 2016/680 (art. 11) e adeguare la normativa nazionale alle disposizioni del RGPD (art. 13), fissando i seguenti principi e criteri direttivi:

ABROGARE espressamente le disposizioni del Codice in materia di trattamento dei dati personali, decreto legislativo 30 giugno 2003, n. 196 (d'ora in poi Codice), incompatibili con le disposizioni contenute nel RGPD;

MODIFICARE il Codice limitatamente a quanto necessario per dare attuazione alle disposizioni non direttamente applicabili contenute nel RGPD e coordinare le disposizioni vigenti in materia di protezione dei dati personali con le disposizioni del RGPD;

PREVEDERE, ove opportuno, il ricorso a specifici provvedimenti attuativi e integrativi adottati dal Garante per la protezione dei dati personali nell'ambito e per le finalità previsti dal RGPD;

ADEGUARE il sistema sanzionatorio, penale e amministrativo, vigente alle disposizioni del RGPD, con previsione di sanzioni penali e amministrative efficaci, dissuasive e proporzionate alla gravità delle violazioni commesse.

Il D.lgs 101/2018 (disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento UE 2016/679) è stato pubblicato in Gazzetta Ufficiale G.U. n. 205 del 04/09/2018

Informatica e didattica s.a.s. – tel. 0982.41460 – e-mail indica@infocima.it