GDPR

A scuola di Privacy con il Regolamento UE 2016/679

dott. Gianluca Apicella Fiorentino

LE FONTI

Regolamento UE 2016/679 del 27 aprile 2016 sulla tutela delle persone fisiche con riferimento al trattamento dei dati personali e alla loro libera circolazione, entrato in vigore il 24 maggio 2016; In quanto Regolamento UE non richiede normativa interna di recepimento e sarà immediatamente applicabile in tutti gli Stati membri a partire dal 25 maggio 2018

CRITICITA': TRADUZIONE DALL'INGLESE

La lingua «madre» del Regolamento Europeo è l'inglese; la traduzione in italiano ha generato molte perplessità e, in alcuni casi, confusione

DECRETO 10 AGOSTO 2018 N. 101

Delega al Governo modifica codice privacy

L. n. 163/2017 art. 13

Alcune novità previste:

- eliminazione di alcune sanzioni penali: ne bis in idem
- Eliminazione del reato di cui all'art. 169 del previgente Codice, "Misure di sicurezza".
- Modalità semplificate di adempimento degli obblighi del titolare del trattamento per le micro, piccole e medie imprese.
- Il minore che ha compiuto i quattordici anni può esprimere il consenso al trattamento dei propri dati personali.
- Previsione di figure intermedie operanti sotto l'autorità del titolare o responsabile
- Periodo transitorio di otto mesi per le sanzioni amministrative

PAROLE CHIAVE

- Dati (personali, particolari e giudiziari)
- Accountability
- Privacy by design
- Privacy by default
- DPO/RPD
- Registri trattamenti
- DPIA
- Incaricati
- Data breach
- Oblio

I DATI

I **dati personali** sono le informazioni che identificano o rendono identificabile una **persona fisica**

- i **dati identificativi**: permettono l'identificazione diretta, come i dati anagrafici, le immagini, ecc.;

- i **dati particolari**: possono rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche o di altro genere, le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale, lo stato di salute e la vita sessuale;

- i **dati giudiziari**: possono rivelare l'esistenza di determinati provvedimenti giudiziari penali (*ad esempio*, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

ACCOUNTABILITY

la responsabilizzazione (*accoutability*) dei titolari del trattamento è il cardine del Regolamento, che genera l'adozione di approcci e politiche preordinate alla valutazione adeguata del rischio che un determinato trattamento di dati personali può comportare per i diritti e le libertà degli interessati.

ACCOUNTABILITY 1

Responsabilità incondizionata in capo a un soggetto del risultato conseguito da un'organizzazione, sulla base delle proprie capacità, abilità ed etica. Tale responsabilità richiede giudizio e capacità decisionale, e si realizza nei confronti di uno o più portatori di interessi con conseguenze positive (premi) o negative (sanzioni), a seconda che i risultati desiderati siano raggiunti o disattesi. L'accento non è posto sulla responsabilità delle attività svolte per raggiungere un determinato risultato, ma sulla definizione specifica e trasparente dei risultati attesi che formano le aspettative, su cui la responsabilità stessa si basa e sarà valutata. La definizione degli obiettivi costituisce, dunque, un mezzo per assicurare l'accountability.

Fonte: treccani.it

ACCOUNTABILITY 2

Insieme al concetto di responsabilità presuppone quelli di trasparenza e di compliance. La prima è intesa come accesso alle informazioni concernenti ogni aspetto dell'organizzazione volto a rendere visibili decisioni, attività e risultati. La seconda si riferisce al rispetto delle norme ed è intesa sia come garanzia della legittimità dell'azione sia come adeguamento dell'azione agli standard stabiliti da leggi, regolamenti, linee guida etiche o codici di condotta. Sotto questi aspetti, l'*accountability* può anche essere definita come l'obbligo di spiegare e giustificare il proprio comportamento.

Fonte: treccani.it

ACCOUNTABILITY 3

Il Regolamento propone la responsabilizzazione (accoutability) dei **titolari del trattamento** e sostiene l'adozione di approcci e politiche che mantengano costantemente alta l'attenzione riguardo al rischio che un determinato trattamento di dati personali possa comportare per i diritti e le libertà degli interessati.

Il titolare del trattamento *deve poter dimostrare policy e processi conosciuti dall'organizzazione* *(Garante)*

PRIVACY BY DESIGN

L'utente è considerato il centro del sistema privacy

Qualsiasi progetto (sia strutturale sia concettuale) va realizzato considerando sin dalla sua progettazione (appunto by design) la riservatezza e la protezione dei dati personali. La **Privacy by Design** comprende una trilogia di applicazioni:

- sistemi IT;
- pratiche (commerciali) corrette;
- progettazione strutturale e infrastrutture di rete.

PRIVACY BY DESIGN 1

Vengono individuati 7 principi fondazionali che esprimono pienamente l'intero senso di questa prospettiva

1. Proattivo non reattivo – prevenire non correggere;
2. Privacy come impostazione di base;
3. Privacy incorporata nella progettazione;
4. Massima funzionalità;
5. Sicurezza fino alla fine − Piena protezione del ciclo;
6. Visibilità e trasparenza − Mantenere la trasparenza;
7. Rispetto per la privacy dell'utente − Centralità dell'utente).

PRIVACY BY DEFAULT

Il principio di *privacy by default* stabilisce che per impostazione predefinita si dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini. Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

Cosa devono fare le Istituzioni Scolastiche?

dott. Gianluca Apicella Fiorentino

INFORMATIVA E CONSENSO

I PRINCIPALI ADEMPIMENTI

- L'INFORMATIVA: art. 13 del Codice – **atto unilaterale da pubblicare**. Occorre una prova dell'avvenuta produzione (ad esempio all'iscrizione o al trasferimento). Se emergono nuove ipotesi di trattamento, a fine anno è opportuno tradurle nell'informativa
- IL CONSENSO: art. 18 del Codice – è un contratto. La Scuola non ha bisogno di consenso, quando versa in attività istituzionale; o il trattamento è lecito e coperto dall'informativa, altrimenti **nessun consenso sana alcunché**.

INFORMATIVA 1

l'informativa: il rapporto con gli interessati (alunni, famiglie, fornitori, personale dipendente) si basa ancora su questo strumento (informative idonee per minori);

I contenuti dell'informativa sono elencati **in modo tassativo** negli articoli 13, paragrafo 1, e 14, paragrafo 1, del regolamento

INFORMATIVA 1

Il titolare **DEVE SEMPRE** specificare nell'informativa:

- i **dati di contatto del RPD-DPO (Responsabile della protezione dei dati-Data Protection Officer);**
- la **base giuridica** del trattamento;
- **qual è il suo interesse legittimo** se quest'ultimo costituisce la base giuridica del trattamento;
- **se trasferisce i dati personali in Paesi terzi** e **attraverso quali strumenti;**
- **il periodo di conservazione dei dati** o i criteri seguiti per stabilire tale periodo di conservazione; il diritto di **presentare un reclamo** all'autorità di controllo.

INFORMATIVA 2

Deve avere forma **concisa, trasparente, intelligibile per l'interessato e facilmente accessibile**; occorre utilizzare un linguaggio **chiaro e semplice.**

Per i minori occorre prevedere informative idonee.

(scritte in un linguaggio semplice e chiaro che un minore possa facilmente capire)

Nel caso di dati personali non raccolti direttamente presso l'interessato *(art. 14 del regolamento)*, 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 o all'interessato.

INFORMATIVA 3

L'informativa deve essere data, **in linea di principio**, **per iscritto** e **preferibilmente in formato elettronico**, soprattutto nel contesto di servizi online; sono comunque ammessi "altri mezzi", quindi può essere fornita anche oralmente.

CONSENSO

consenso/autorizzazione: non serve per la stragrande maggioranza dei trattamenti perché sono le norme che individuano gli ambiti dei trattamenti stessi – il regolamento prevede il diritto di opposizione che la PA può neutralizzare con adeguata motivazione;

DATI NON SENSIBILI

principio di necessità:

trattare dati non sensibili solo se necessario per il lavoro della scuola, possibilmente con sistemi di pseudonimizzazione o anonimizzazione

DATI SENSIBILI

trattare dati sensibili, solo se indispensabili per lavorare o fornire un servizio espressamente richiesto, se lo prevede il DM 305/2006, se è proprio necessario, in linea con art. 9 Regolamento UE;

richiamare in via cautelare il principio di indispensabilità negli ambiti definiti dal DM 305/2006

WEB

Per pubblicare sul web, dobbiamo riferirci ad una norma di legge o di regolamento che lo consenta (ad es. trattamento temporaneo finalizzato esclusivamente alla pubblicazione o diffusione occasionale di articoli, saggi e altre manifestazioni del pensiero anche nell'espressione artistica art. 136 c. 1 lett. c Dlgs 196/2003); ovviamente solo per gli scopi istituzionali dell'ente.

Stesso criterio per foto e video, comunicati o diffusi in qualunque altra modalità (informativa, motivazione, principio di necessità, riferimenti normativi)

SICUREZZA 1

Le misure di sicurezza passano da «minime» ad «adeguate»

Art. 32 del Regolamento UE

Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell' oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative **adeguate** per garantire un livello di sicurezza **adeguato** al rischio, che comprendono, tra le altre, se del caso: **pseudonimizzazione, riservatezza sistemi di trattamento, capacità di ripristino sistemi compromessi, valutazione continua possibili vulnerabilità, ecc.**

SICUREZZA 2

Attenersi, in attesa di nuove indicazioni, alle precedenti (attuali) misure minime di sicurezza (Art. 33, 34, 35 del codice e Allegato B del Dlgs 196/2003), di cui al livello «M» dell'allegato alla Circolare AgID n. 2/2017

MISURE DI SICUREZZA: RISCHI

distruzione, perdita, modifica, divulgazione non autorizzata, derivanti dall'accesso in modo accidentale o illegale

TITOLARE E RESPONSABILE DEL TRATTAMENTO

Il **«titolare del trattamento»** (controller) è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali;

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

IL RESPONSABILE DEL TRATTAMENTO 1

Quando e chi nominare Responsabile del Trattamento interno e esterno (ad esempio ditta che effettua assistenza) con un suo registro dei trattamenti?

E' il titolare che designa il responsabile iniziale del trattamento; quest'ultimo potrà eventualmente designare altri responsabili del trattamento.

Il RTD dovrà fornire le "garanzie sufficienti" per mettere in atto le misure tecniche ed organizzative adeguate nonché garantisca la tutela dei diritti dell'interessato.

IL RESPONSABILE DEL TRATTAMENTO 2

la nomina deve avvenire tramite contratto o altro "*atto giuridico a norma del diritto dell'Unione o degli Stati membri*, *che vincoli il responsabile del trattamento al titolare del trattamento e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare del trattamento*".

Il Responsabile ha **obblighi di trasparenza, di garantire la sicurezza dei dati e di avvisare, assistere e consigliare il titolare**

IL RESPONSABILE DEL TRATTAMENTO 3

Chiunque gestisca un servizio (cloud e non) e tratti i dati per conto della scuola è giuridicamente il Responsabile del Trattamento dei Dati; deve essere **GDPR Compliance,** deve conservare il registro dei trattamenti effettuati per conto della scuola cliente (titolare del trattamento) e ha l'obbligo di notificare al titolare le eventuali violazioni di dati.

Quando il servizio non ha natura occasionale la nomina a responsabile è **obbligatoria**

AUTORIZZATO AL TRATTAMENTO

Quando e chi nominare Autorizzato o Incaricato del trattamento con riferimento agli artt. 29 e 32 del Regolamento riguardo ai **soggetti istruiti**, (docenti, assistenti amministrativi, ecc.).

Il Regolamento consente di differenziare livelli di autorizzazione e istruzioni

PRIVACY O TRASPARENZA?

In attesa di ulteriori indicazioni continuare a bilanciare privacy e trasparenza, riferendosi alla normativa in vigore e non in contrasto con il regolamento, con riferimento a:

- accesso agli atti (L.241/90)
- accesso civico/generalizzato (Dlgs 33/2013)
- indicazioni di ANAC, circolari, Giurisprudenza, Garante, ecc.)

Per la pubblicazione dei dati personali proseguire come fatto finora su Amministrazione Trasparente (Dlgs 33/2013) e sull'Albo on line (Linee guida AGID 2016)

IL CUORE DEL REGOLAMENTO 1

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 art. 30, paragrafo 5)*, devono tenere un registro delle operazioni di trattamento; è uno **strumento fondamentale** ai fini dell'eventuale supervisione da parte del Garante e per disporre di un quadro aggiornato dei trattamenti in essere all'interno della scuola – **indispensabile per ogni valutazione e analisi del rischio**.

Si aggiorna al mutare degli elementi essenziali, non si pubblica.

IL CUORE DEL REGOLAMENTO 2

Inoltre non dovrebbe necessariamente trattarsi di un mero obbligo; la redazione del registro potrebbe essere ispirata alle seguenti ulteriori finalità:

rappresentare l'organizzazione sotto il profilo delle attività di trattamento a fini di informazione, consapevolezza e condivisione interna;

costituire lo strumento di pianificazione e controllo della politica della sicurezza di dati e banche di dati, tesa a garantire la loro integrità, riservatezza e disponibilità.

VALUTAZIONE D'IMPATTO DPIA

Quando un trattamento può comportare un rischio elevato per i diritti e le libertà delle persone interessate il **regolamento 2016/679** obbliga i titolari a svolgere una **valutazione di impatto** prima di darvi inizio, consultando l'autorità di controllo in caso le misure tecniche e organizzative da loro stessi individuate per mitigare l'impatto del trattamento non siano ritenute sufficienti - cioè, quando il rischio residuale per i diritti e le libertà degli interessati resti elevato.

VALUTAZIONE D'IMPATTO DPIA 2

è un sistema di gestione vincolato a rischi elevati di violazione di diritti e libertà fondamentali.

I principi privacy by design e privacy by default esigono comunque un' analisi dei rischi standard, prevista nel registro dei trattamenti).

Non è tra le priorità per la PA indicate dal Garante in sede di prima applicazione del Regolamento (le autorità Garanti stanno lavorando sull' elenco delle attività soggette a DPIA, sui codici di condotta, sistemi di certificazione, ecc.

RPD /DPO

La nomina del responsabile della protezione dati (RPD) o Data Protection Officer (DPO) è una delle vere novità del regolamento e va comunicata al Garante

La funzione del RDP è quella di vigilare in via generale sui trattamenti posti in essere dal titolare

I DPO deve essere tempestivamente e adeguatamente coinvolto in tutte le questioni inerenti la protezione dei dati nonché sostenuto nell'esecuzione dei suoi compiti dal titolare e dal responsabile del trattamento;

RPD /DPO 2

L'articolo 39 del Regolamento specifica nel dettaglio quali sono i compiti minimi del DPO:

- informare e fornire consulenza al titolare e al responsabile del trattamento in merito agli obblighi derivanti dal Regolamento o dalle altre disposizioni legislative interne o europee in materia di protezione dati;
- sorvegliare l'osservanza del Regolamento da parte del titolare e del responsabile del trattamento
- fornire su richiesta pareri in merito alla valutazione d'impatto e sorvegliarne lo svolgimento;
- cooperare con l'autorità di controllo fungendo da punto di contatto per questioni connesse al trattamento, effettuando consultazioni di ogni tipo, con particolare riguardo e attenzione ad un'eventuale attività di consultazione preventiva.

DATA BREACH

I titolari del trattamento dovranno **documentare le violazioni** di dati personali subite e in alcuni casi notificarle all'autorità di controllo indicando le relative circostanze e conseguenze e i provvedimenti adottati *(art. 33, paragrafo 5); devono poter* fornire tale documentazione, su richiesta, al Garante in caso di accertamenti (vedi modulistica presente nel sito del Garante).

IL REGISTRO DELLE VIOLAZIONI

Il registro delle violazioni di cui all'articolo 33 del Regolamento documenta i casi di violazione effettivamente occorsi ma può anche contemplare le minacce potenziali, per identificare il tipo e la natura delle violazioni più ricorrenti.

In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche.

Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo.

Dott. Gianluca Apicella Fiorentino

IL REGISTRO DELLE VIOLAZIONI

Occorre registrare tutte le violazioni della sicurezza che comportano 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**.**

In alcuni casi comunicazione anche agli interessati (no se misure adeguate e se ci sono rischi minori e se comunicazione sproporzionata).

CASI

- ■TEMI IN CLASSE: non ci sono particolari prescrizioni nemmeno per la lettura in classe dei temi, se non il segreto d'ufficio e professionale
- VOTI ED ESAMI: gli esiti degli esami di Stato sono pubblici. Le "prove differenziate" non vanno indicate nei tabelloni, ma solo in certificazione
- COMUNICAZIONI SCUOLA-FAMIGLIA: nelle comunicazioni non dirette a specifici destinatari evitare dati personali (es. vicende di bullismo)
- DISABILITÀ E DSA: sono dati sensibili, mai oggetto di diffusione
- MENSA: questione di competenza degli enti locali, per lo più: convinzioni religiose e dati sanitari relativi ai regimi alimentari

CASI 1

- SCUOLA-LAVORO: eccezionalmente, occorre il consenso degli alunni per la comunicazione a terzi (imprese incluse) dei dati relativi al loro rendimento
- CURRICULUM E IDENTITÀ DIGITALE DELLO STUDENTE: …
- SMARTPHONE E TABLET: un conto è la possibilità astratta di usare la strumentazione tecnologica, un altro conto è l'eventuale Regolamento interno che ne inibisce l'uso a scuola. Resta responsabile dell'eventuale diffusione il soggetto che la mette materialmente in essere
- RECITE E VIAGGI DI ISTRUZIONE: nessuna questione di riservatezza, se non intermini di eventuale diffusione, per la quale vale il punto precedente
- REGISTRAZIONE DELLE LEZIONI: DSA a parte / vietabile in Regolamento interno / della diffusione resta responsabile l'autore materiale

CASI 2

- GRADUATORIE DEL PERSONALE E SUPPLENZE: sono pubbliche per legge, ma soggette al principio di necessità. Dunque nome, cognome, punteggio eposizione in graduatoria, ma non numeri di telefono e/o indirizzi
- PAGAMENTO DEL SERVIZIO MENSA O ALTRI EMOLUMENTI SCUOLA: vietata la pubblicazione dell'elenco dei morosi. Buoni pasto di colore differente sono da evitare
- SCUOLABUS: vietato pubblicare gli elenchi degli utenti o i percorsi
- VIDEOSORVEGLIANZA: si può fare, ma:
- – solo le aree interessate – solo negli orari di chiusura
- – perimetro: anche durante l'orario – cartelli

CASI 3

- QUESTIONARI PER ATTIVITÀ DI RICERCA: attività possibile previa informativa, non può avere carattere obbligatorio
- MARKETING E ATTIVITÀ COMMERCIALI: … e la finalità istituzionale ?
- IL "FRONTE" SOCIAL NETWORK E INSTANT MESSAGING:
- – ricordare il principio di necessità
- – presenza della scuola e dei singoli dipendenti
- – gruppi di IM: occhio alle EULA End User License Agreement
- – … ricordare il principio di necessità!