GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

Regolamento Privacy Unione Europea (2016/679) relativo al trattamento dei dati personali dei cittadini della Comunità Europea

Renato Narcisi – NetSense S.r.l.

GDPR coinvolge privacy e protezione dei dati

TUTELA DELLA PRIVACY:
riservatezza nell'uso delle informazioni personali di terzi

PROTEZIONE DEI DATI:
obblighi relativi alle misure di sicurezza nella gestione informatica dei dati

SOLO dati di persone fisiche: non si applica ai dati delle persone giuridiche

cosa è cambiato? Accountability nel GDPR

Il regolamento introduce il principio della
accountability ("dover rendere conto del proprio operato")

NESSUNA LISTA DI COSE DA FARE:
si demanda ai titolari il compito di decidere autonomamente
le modalità e i limiti del trattamento dei dati

RESPONSABILIZZAZIONE
LE MISURE DA ADOTTARE SONO A DISCREZIONE DEL TITOLARE
SERVE **ADOTTARLE** E **DOCUMENTARLE**

cosa evitare? il Data Breach (art. 33, C85, C87, C88)

Data Breach: **violazione degli standard di sicurezza adottati per la protezione dei dati personali** che può comportare "accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, memorizzati o comunque trattati".

- Accesso non autorizzato a risorse informatiche
- Cancellazione totale o parziale di archivi
- Furto di identità
- Diffusione volontaria o involontaria di dati sensibili
- Accesso a siti web non consentiti
- Alterazione di database
- Intrusione fisica in strutture ad accesso riservato
- Installazione di software potenzialmente dannosi
- Utilizzo di risorse aziendali per cyber attacchi a sistemi di terzi
- Violazione di copyright
- Denial of service

→ Attenzione alle linee guida sulla sicurezza ICT emanate dall'AGID (circolare 2/2017)

cosa evitare? il Data Breach (art. 33, C85, C87, C88)

In caso di data breach è necessaria la comunicazione all'autorità di vigilanza entro 72 ore.

Esiste la possibilità, giudicando l'evento non grave, di predisporre una determina dirigenziale dichiarando i motivi per non procedere alla segnalazione.

E' anche necessario **riportarlo nel "Registro dei trattamenti"** o in un suo allegato.
Teneteci informati di ogni evento. Lo aggiorneremo noi, per vostra comodità.

Si tratta di una vera e propria auto-denuncia, nella quale è importante indicare le misure che si intende adottare nel futuro per non incorrere più nella stessa problematica.

BISOGNA FARE IL POSSIBILE PER EVITARE I DATA BREACH !!!

GDPR - General Data Protection Regulation

RGPD - Regolamento Generale sulla Protezione dei Dati

FIGURE E RUOLI DELLA NORMATIVA

art. 4 - Figure e ruoli previsti dalla normativa

DEFINIZIONE ITALIANA	CHI E' / SONO ?
Titolare del trattamento	La Scuola nella persona del DS
Interessati	I proprietari dei dati
Addetti al trattamento	I dipendenti della scuola
Responsabili del trattamento	I fornitori (sotto particolari condizioni)
Responsabile della protezione dei dati	Il DPO

Da normative precedenti ma non espressamente indicate dal GDPR

Amministratore di sistema / di rete / di database

Scompare l'incaricato del Trattamento

prima di tutto: base giuridica per i trattamenti delle PA

CONSENSO? NO!

sin dai lavori preparatori del Codice privacy italiano alla Camera

Primo step della “storia”:

Art.6 del Regolamento elenca le basi giuridiche. Tra queste, il consenso è annoverato.

Articolo 6

Liceità del trattamento

1. Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: (**C40**)

a) l’interessato ha espresso il consenso al trattamento dei propri dati personali per una o più specifiche finalità; (**C42, C43**)

b) il trattamento è necessario all’esecuzione di un contratto di cui l’interessato è parte o all’esecuzione di misure precontrattuali adottate su richiesta dello stesso; (**C44**)

c) il trattamento è necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento; (**C45**)

d) il trattamento è necessario per la salvaguardia degli interessi vitali dell’interessato o di un’altra persona fisica; (**C46**)

e) il trattamento è necessario per l’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri di cui è investito il titolare del trattamento; (**C45, C46**)

f) il trattamento è necessario per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell’interessato che richiedono la protezione dei dati personali, in particolare se l’interessato è un minore. (**C47-C50**)

prima di tutto: base giuridica per i trattamenti delle PA

comma (paragrafo) 2 art. 6 Regolamento

2. Gli Stati membri possono mantenere o introdurre disposizioni più specifiche per adeguare l'applicazione delle norme del presente regolamento con riguardo al trattamento, in conformità del paragrafo 1, lettere c) ed e), determinando con maggiore precisione requisiti specifici per il trattamento e altre misure atte a garantire un trattamento lecito e corretto anche per le altre specifiche situazioni di trattamento di cui al capo IX. (**C8, C10, C41, C45, C51**)

comma (paragrafo 3) art. 6 Regolamento

3. La base su cui si fonda il trattamento dei dati di cui al paragrafo 1, lettere c) ed e), deve essere stabilita: (**C8, C10, C41, C45, C51**)

a) dal diritto dell'Unione; o

b) dal diritto dello Stato membro cui è soggetto il titolare del trattamento.La finalità del trattamento è determinata in tale base giuridica o, per quanto riguarda il trattamento di cui al paragrafo 1, lettera e), è necessaria per l'esecuzione di un compito svolto nel pubblico interesse o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento. Tale base giuridica potrebbe contenere disposizioni specifiche per adeguare l'applicazione delle norme del presente regolamento, tra cui: le condizioni generali relative alla liceità del trattamento da parte del titolare del trattamento; le tipologie di dati oggetto del trattamento; gli interessati; i soggetti cui possono essere comunicati i dati personali e le finalità per cui sono comunicati; le limitazioni della finalità, i perio-

base giuridica: scelta dell'Italia

Secondo step della "storia":
la scelta del legislatore italiano

Adottare maggiore specificità riguardo le basi giuridiche dei trattamenti effettuate dalle PA

art.2-ter del Codice privacy (196/2003 mod. 101/2018):

Art. 2-ter (Base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri)

1. La base giuridica prevista dall'articolo 6, paragrafo 3, lettera b), del regolamento e' costituita esclusivamente da una norma di legge o, nei casi previsti dalla legge, di regolamento.

2. La comunicazione fra titolari che effettuano trattamenti di dati personali, diversi da quelli ricompresi nelle particolari categorie di cui all'articolo 9 del Regolamento e di quelli relativi a condanne penali e reati di cui all'articolo 10 del Regolamento, per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri e' ammessa se prevista ai sensi del comma 1. In mancanza di tale norma, la comunicazione è ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico e lo svolgimento di funzioni istituzionali e puo' essere iniziata se e' decorso il termine di quarantacinque giorni dalla relativa comunicazione al Garante, senza che lo stesso abbia adottato una diversa determinazione delle misure da adottarsi a garanzia degli interessati.

3. La diffusione e la comunicazione di dati personali, trattati per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, a soggetti che intendono trattarli per altre finalita' sono ammesse unicamente se previste ai sensi del comma 1.

4. Si intende per:

a) "comunicazione", il dare conoscenza dei dati personali a uno o piu' soggetti determinati diversi dall'interessato, dal rappresentante del titolare nel territorio dell'Unione europea, dal responsabile o dal suo rappresentante nel territorio dell'Unione europea, dalle persone autorizzate, ai sensi dell'articolo 2-*quaterdecies*, al trattamento dei dati personali sotto l'autorita' diretta del titolare o del responsabile, in qualunque forma, anche mediante la loro messa a disposizione, consultazione o mediante interconnessione;

b) "diffusione", il dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione.

base giuridica: scelta dell'Italia

In sintesi, quindi, la base giuridica per i trattamenti delle PA
è data SEMPRE E SOLO da una norma di legge o di regolamento.
Quindi: NESSUN CONSENSO

E allora? I genitori non sono tutelati?
Al contrario!!!

Oltre al classico dovere informativo (INFORMATIVA ARTT. 13 e 14),
l'assenza dell'istituto del consenso impone a noi scuole un carico in più:

individuare per ogni trattamento la norma che lo regola
(e, conseguentemente, gestire il diritto di opposizione delle famiglie)

esempio: trasmissione esiti formativi (art. 96 del Codice privacy)

Art. 96 *(Trattamento di dati relativi a studenti)*

1. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonche' le istituzioni di alta formazione artistica e coreutica e le universita' statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità.

2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.

art. 96 come “appoggio” per foto e video? NO!

Estratto documento Audit alla camera (pag.17)

Atti del governo

L’adeguamento della disciplina sulla protezione dei dati personali al Regolamento (UE) 2016/679

18 Giugno 2018

Articolo 7 ***Modifiche alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196***	
l. Alla Parte II, Titolo VI, del decreto legislativo 30 giugno 2003, n. 196, l'articolo 96 è sostituito dal seguente: "Art. 96 (*Trattamento di dati relativi a studenti*) 1. Al fine di agevolare l’orientamento, la formazione e l’inserimento professionale, anche all’estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute su richiesta degli interessati, possono comunicare o diffondere, anche a privati e per via telematica, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali diversi da quelli di cui agli articoli 9 e 10 del Regolamento, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell’articolo 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità. 2. Resta ferma la disposizione di cui all'articolo 2, comma 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati.”	**ANP (Dirigenti scolastici)**: chiede un’integrazione all’art. 96, affinché previa adeguata informativa agli interessati e nel rispetto del principio di minimizzazione dei trattamenti, con rigorosa selezione da parte della scuola, sia chiaramente consentito alle scuole l’uso di foto ed immagini anche attraverso forme di pubblicazione sul sito istituzionale.

GESTIONE DELLA PRIVACY NEI RAPPORTI CON LE FAMIGLIE

PRASSI E DOCUMENTAZIONE DA PRODURRE

documentazione GDPR – “faldone privacy”

- **Registro dei trattamenti** **(NB: tutti i trattamenti ivi elencati devono trovare indicazione nelle varie informative)**
- Modulo diritto accesso (**)
- Modulo diritto opposizione (**)
- Modulo segnalazione data breach (**)

Famiglie

- Informativa generale con modulo di presa visione (**)
- Moduli per partecipazione a progetti didattici della scuola (Informativa specifica e richiesta)
- Moduli per partecipazione a progetti/concorsi organizzati da terzi
- Moduli per osservazioni in aula da professionisti incaricati da una famiglia
- Cartello per foto realizzate dai genitori
- Moduli per foto fine anno con fotografo
- Liberatoria immagini per TV e giornali
- Modulo per richiesta comunicazione esiti (art.96 Codice privacy)
- Disclaimer DAD
- Altre informative specifiche con appositi moduli di presa visione

Legenda: (**) pubblicati su sito

documentazione GDPR – “faldone privacy”

Legenda: (**) pubblicati su sito

Dipendenti

- Informativa generale ai dipendenti (**)
- Atto organizzativo e piano di protezione privacy
- Autorizzazioni ed istruzioni personale ATA amministrativo e DSGA (nasce da atto organizzativo)
- Autorizzazioni ed istruzioni personale docente e tirocinanti (“ ”)
- Autorizzazioni ed istruzioni personale collaboratori scolastici (“ ”)
- Autorizzazioni ed istruzioni personale tecnico e/o animatore digitale (“ ”)
- **Prese visione delle informative, dell’atto autorizzativo e delle istruzioni (IMPORTANTE)**
- Disposizioni DAD - Regolamento (?)

Fornitori

- Informativa generale ai fornitori (**)
- TUTTE le nomine a “responsabile del trattamento” (IMPORTANTI) ai fornitori/consulenti che trattano dati per conto della scuola e che siano assoggettati nella scelta delle finalità
- Accordi di contitolarità con i fornitori/consulenti che trattano dati per conto della scuola con proprie finalità e che condividano con la scuola i trattamenti.