

IMPATTO G.D.P.R. NELLA DIDATTICA QUOTIDIANA

General Data Protection Regulation

Regolamento generale sulla protezione dei dati

‘dal 25 maggio 2018, il GDPR deve essere pienamente e integralmente attuato, anche se non è ancora stato adottato il decreto delegato di adeguamento’

Fonti principali:

https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection_it

<https://www.schooleducationgateway.eu/it/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm>



Un'amministrazione pubblica è soggetta alle norme del GDPR quando tratta i **dati personali** di una persona.

Generalmente, la maggior parte dei dati personali detenuti dalle amministrazioni pubbliche è trattata sulla base di un **obbligo giuridico o nella misura in cui ciò è necessario per eseguire compiti svolti nell'interesse pubblico** o per l'esercizio di un'autorità ufficiale a esse conferita.

I **dati personali** sono tutte le informazioni che possono identificare una persona o la sua famiglia. Nei documenti scolastici, questi dati sono **nome, indirizzo, informazioni di contatto, registro scolastico disciplinare, voti e schede di valutazione**. Questo tipo di dati resta “personale” anche se un individuo sceglie di renderli pubblici.

Una **categoria speciale** di dati attiene a questioni più sensibili. Nel caso delle scuole, queste comprendono **dati biometrici** (es. impronte digitali, foto), **credo religioso** (es. la scelta di non seguire le ore di religione), **salute** (es. allergie) o **prescrizioni alimentari** (che possono dare indicazioni su fede religiosa o stato di salute). I dati appartenenti a questa categoria possono quindi essere elaborati solo a determinate condizioni. Le scuole non li possono utilizzare senza il consenso dei genitori degli alunni.

Nel trattare i dati personali, l'amministrazione pubblica è tenuta ad assicurarsi di rispettare principi fondamentali come:

- trattamento corretto e lecito;
- limitazione delle finalità;
- **minimizzazione** e conservazione dei dati.

Prima di trattare i dati personali, è necessario informare le persone in merito al trattamento: **le sue finalità**, i tipi di dati raccolti, i destinatari e i loro diritti di protezione dei dati.

Una amministrazione pubblica è tenuta a **nominare un responsabile della protezione dei dati**; tuttavia, è possibile designare un unico responsabile della protezione dei dati per diversi organismi pubblici.

Nel nostro istituto è l'ing. Maurizio Felici.

Deve inoltre assicurarsi di aver attuato misure tecniche e organizzative adeguate per **proteggere i dati personali**.

Nei casi in cui i dati personali raccolti siano divulgati accidentalmente o illegalmente a destinatari non autorizzati o siano temporaneamente indisponibili o alterati, **occorre notificare la violazione all'autorità per la protezione dei dati** senza indebito ritardo e al più tardi entro 72 ore dal momento in cui si è venuti a conoscenza della violazione. Potrebbe anche essere necessario informare le persone della violazione o perdita.

I dati non possono essere riciclati ad altri fini. Per esempio, la scuola non può condividere l'indirizzo mail di un genitore con terze parti che promuovano eventi scolastici affermando che si tratta di "interesse pubblico". Per condividere questo dato, infatti, la scuola deve rifarsi a un'altra base giuridica, **il consenso**. Le scuole devono chiedere il consenso anche per aprire un account-studente su un servizio di cloud-hosting.

I furti di dati non sono sempre opera di hacker e software maligni, ma possono anche essere il frutto di un portatile o una chiavetta USB dimenticati in un luogo pubblico o in auto, della curiosità di un membro della famiglia o di uno smarrimento involontario.

Per questa ragione, il personale scolastico deve conservare i dati personali solo su attrezzature informatiche o aree dati protette di proprietà della scuola, usare password forti e impostare il blocco automatico del dispositivo dopo cinque minuti di inattività. Se i dati personali vengono scaricati su un supporto mobile come una chiavetta USB, questo deve essere criptato e protetto da password, e tenuto al sicuro..

Principali misure che metteremo subito in atto:

1. Aggiornamento (entro gennaio 2020) di tutti i PC a Windows 10.
2. Chi attua progetti scolastici che hanno finalità extracurricolari o che prevedono il coinvolgimento di soggetti esterni dovrà predisporre e richiedere espressa autorizzazione privacy ai genitori.
3. A ciascun docente e studente (previa autorizzazione) verrà distribuito un account Google Education che dovrà essere obbligatoriamente utilizzato per tutte le attività didattiche o per le comunicazioni che contengono dati di alunni.