LA PRIVACY NELLA SCUOLA

Nota per docenti e figure in compresenza durante le lezioni

Dott. Pier Giorgio Galli

Principali fonti normative

- Regolamento Generale sulla Protezione dei dati - GDPR (UE) 2016/679
- Codice Privacy - D.lgs 196/2003 e successive modificazioni
- Provvedimenti del Garante per la Protezione dei dati Personali www.garanteprivacy.it

Cosa si intende per trattamento dei dati personali?

Qualsiasi operazione applicata ai dati personali, come ad esempio: la raccolta, la registrazione, l'organizzazione, la conservazione, l'adattamento o la modifica, l'estrazione, **la consultazione**, l'uso, la comunicazione, la diffusione (o pubblicazione), il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione...

Quali sono i dati personali comuni?

I **dati comuni** sono**:** nome, cognome, data di nascita, telefono, indirizzo di posta elettronica, indirizzo abitazione, ISEE, immagini e riprese video, vocali, il codice fiscale, ecc.

Scritta al contrario

NON SONO DATI SENSIBILI:

- il numero di telefono,
- la data di nascita,
- il codice fiscale,
- le immagini,
- ecc.

Quali sono i dati personali sensibili?

I **dati sensibili** (il termine corretto è Categorie particolari di dati) sono **solo** questi:

1. dati relativi alla salute,
2. dati relativi alla vita sessuale o all'orientamento sessuale (es. carriera alias degli studenti),
3. dati relativi all'origine razziale o etnica,
4. dati relativi alle opinioni politiche,
5. dati relativi alle convinzioni religiose, filosofiche o all'appartenenza sindacale,
6. dati genetici, dati biometrici.

Quali sono i dati personali giudiziari?

I **dati giudiziari** (il termine corretto è dati personali relativi a condanne penale e reati) che potrebbero interessare la scuola sono ad esempio:

1. sentenze di allontanamento dei genitori,
2. sentenze in merito a genitori che possono avere contatti con i figli solo in determinati giorni della settimana,
3. sentenze che riguardano condanne degli studenti
4. visure presso il casellario giudiziario (segreteria),
5. studenti soggetti a regime di protezione, ecc.
6. ecc.

Chi sono le figure coinvolte?

- **Titolare del trattamento** - L'Istituzione Scolastica legalmente rappresentata dal Dirigente Scolastico
- **Responsabile della protezione dei dati (DPO)** - Pier Giorgio Galli
- **Responsabili del trattamento dei dati** – Argo, Axios, Spaggiari… (Registro elettronico), Google (Google Workspace), Microsoft (Microsoft 365),…
- **Autorizzati a trattare i dati personali** – personale scolastico
- **Interessati dal trattamento** - Studenti, genitori, personale scolastico, visitatori della scuola, fornitori, utenti del sito web…

Cosa sono l'informativa e l'autorizzazione?

L'informativa è un documento destinato agli interessati del trattamento (personale scolastico, famiglie, fornitori, ecc.) che descrive le modalità con cui i loro dati personali vengono trattati e quali sono i loro diritti. **Le informative sono disponibili nella sezione privacy del sito web della scuola.**

L'autorizzazione per il trattamento dei dati personali è rivolta al **personale scolastico**. Essa include le istruzioni per il trattamento dei dati e le misure di sicurezza da adottare. Viene trasmessa formalmente dal Titolare del trattamento tramite posta elettronica, attraverso il registro elettronico o consegnata a mano.

Il personale scolastico può trattare i dati personali degli alunni? Anche quelli relativi alla salute?

Sì, il personale scolastico può trattare **tutte le tipologie dei dati personali** degli alunni **compresi quelli sulla salute** quando il trattamento **è necessario** per l'espletamento della propria funzione.

Non è necessaria la liberatoria

Le tipologie di trattamento e le specifiche istruzioni su come vanno effettuati sono puntualmente indicati nell'**autorizzazione al trattamento dei dati**.

A chi possono essere comunicati i dati personali?

I dati personali degli studenti possono essere sempre comunicati al Dirigente Scolastico, ai docenti della classe di pertinenza, al personale coinvolto nella filiera educativa, ai genitori (**ma non ai nonni, ai fratelli, …**). In alcuni contesti possono essere comunicati anche ad agenzie esterne per l'organizzazione di visite didattiche, contest, ecc.

È ammessa la delega.

Come vanno trattati i dati personali su supporto cartaceo?

I dati personali su supporto cartaceo non devono mai essere lasciati incustoditi. **Devono essere conservati all'interno di cassetti o armadi chiusi a chiave nei locali della scuola**, oppure, se posti al di fuori di tali contenitori, in ambienti presidiati o con la porta chiusa a chiave.

Che accortezze bisogna porre in atto nelle stampe di documenti contenenti dati personali?

Nel caso in cui la stampa di dati personali avvenga tramite stampanti ad uso collettivo (ad esempio, stampanti in sala professori o fotocopiatrici multifunzione nei corridoi), è fondamentale raccogliere **immediatamente** i documenti stampati e verificare che tutte le pagine siano state correttamente prodotte.

Questo controllo deve essere effettuato anche al termine della fotocopiatura di dati personali.

Possono essere affissi elenchi o immagini di studenti o di docenti nelle bacheche o nei corridoi?

No. Le immagini e gli elenchi di studenti o docenti (ad esempio orari di servizio o sostituzioni) non possono essere esposti in aree accessibili a persone esterne non autorizzate al trattamento dei dati, come corridoi o atrii.
Nei casi in cui l'affissione **sia autorizzata dai genitori** o resa obbligatoria da normative vigenti, sarà il Titolare del trattamento a disporne l'affissione.
Tuttavia, in aree con accesso riservato come le sale professori o all'interno delle aule, l'affissione è consentita.

È consentito lasciare i fogli firma in vista all'ingresso?

No. I fogli firma non devono essere visibili a persone non autorizzate. Se le firme vengono raccolte nell'atrio o nei corridoi, il registro deve essere coperto o posizionato a faccia in giù, in modo che non sia immediatamente visibile.

Tuttavia, nelle aree ad accesso riservato, come le sale docenti, i fogli firma possono essere lasciati in vista.

Che caratteristiche devono avere le password?

Premesso che l'autenticazione tramite SPID e sistemi simili è intrinsecamente sicura e da preferire, nei casi in cui l'accesso avviene tramite nome utente e password è necessario adottare misure di sicurezza per ridurre il rischio di accesso non autorizzato ai dati personali. Le password:

1. devono essere composte da almeno **8 caratteri** e includere elementi di complessità (almeno una lettera maiuscola, una minuscola, un numero e un carattere speciale). Non devono contenere parti del nome, data di nascita o nomi di familiari, né porzioni di essi;
2. vanno rinnovate almeno ogni **tre mesi** senza riusare password simili alle precedenti;
3. **non devono mai essere memorizzate nei browser o in applicazioni simili.**
4. non devono mai essere rivelate a nessuno. Solo in situazioni di emergenza, la password può essere temporaneamente condivisa con un collega fidato, ma va immediatamente rinnovata al termine dell'urgenza.

Come è possibile ricordare tutte le password?

Ricordare tutte le password è dura!

Una soluzione potrebbe essere:

1. organizzare un documento MS Word o Libre Office Writer su cui memorizzare le tutte le password;
2. proteggere il documento con una password (da ricordarsi a memoria);
3. memorizzare il documento protetto contenente le password dispositivi locali o nel cloud.

Come backup stampare su carta il documento e la password e conservarli a casa in un luogo sicuro.

Quali sono le principali misure minime per il trattamento dei dati personali con dispositivi digitali?

1. il trattamento dei dati personali può avere inizio solo dopo aver verificato che l'antivirus e il firewall siano aggiornati e operativi;
2. durante il trattamento vanno posti in atto in atto tutti gli accorgimenti tali da nascondere i dati alla vista di terzi non autorizzati;
3. è fatto divieto di consentire ad altri il trattamento dei dati dopo aver avviato il trattamento con le proprie credenziali di autenticazione;
4. al termine del trattamento o in caso di allontanamento temporaneo deve essere eseguita l'operazione di logout;
5. **la memorizzazione dei dati personali nelle memorie locali dei dispositivi della scuola ad uso collettivo (ad esempio, computer delle aule e dei laboratori) non è mai consentita;**
6. i documenti contenenti dati personali possono essere memorizzati nelle memorie dei dispositivi solo in cartelle **a cui non abbiano accesso altri utenti** dello stesso dispositivo;

Quali sono le principali misure minime per il trattamento dei dati personali con dispositivi digitali?

7. il trattamento dei dati personali su piattaforme on line può avere inizio solo dopo la fornitura delle proprie credenziali di autenticazione ad uso esclusivo;
8. l'uso di chiavette USB o dispositivi simili per la conservazione dei dati personali è consentito, anche al di fuori dell'Istituzione Scolastica. In tal caso, è necessario garantire che il dispositivo sia fisicamente assicurato a un bene personale, come ad esempio le chiavi di casa, in modo che la sua eventuale perdita venga segnalata tempestivamente;

Fare riferimento all'autorizzazione per maggiori info sulle misure minime di sicurezza informatiche da porre in atto.

È possibile utilizzare strumenti on line per modificare documenti PDF che contengono dati personali?

No, mai, nel momento in cui il documento PDF contenete i dati personali viene caricato nella piattaforma cloud è **immediatamente nella disponibilità del gestore della piattaforma**! Lo stesso vale per servizi on line in cui carichiamo immagini di persone per manipolarle.

Per la gestione dei PDF si suggerisce l'applicazione locale https://www.pdf24.org/it/

Quali caselli e-mail possono essere usate?

Per la trasmissione alla scuola di testi o allegati contenenti dati personali (praticamente tutti), è obbligatorio utilizzare esclusivamente:

- **la casella di posta istituzionale della scuola**, tipicamente: nome.cognome@nomescuola.edu.it
- **la casella di posta istituzionale ministeriale**: nome.cognome@scuola.istruzione.it

L'utilizzo di caselle di posta elettroniche personali è di norma evitato per attività o comunicazioni afferenti il servizio, salvi i casi di forza maggiore dovuti a circostanze in cui il dipendente, per qualsiasi ragione, non possa accedere all'account istituzionale» (Codice di comportamento dei dipendenti pubblici – DPR 62/2013).

Cosa è la pseudonimizzazione?

La pseudonimizzazione è una tecnica per mantenere in sicurezza **i dati sensibili**, tipicamente **della salute**, degli studenti come ad esempio per gli studenti con disabilità o con DSA o con BES per motivi di salute (**ricorda il disagio sociale non è un dato sensibile**, per i PDP per questi motivi non è obbligatoria la pseudonimizzazione).
In questi casi allo studente viene associato un codice da utilizzarsi nei documenti scolastici al posto del cognome e nome.

Ricorda, l'uso delle iniziali non è ammesso dal Garante Privacy

Chi gestisce il registro degli pseudonimi?

La gestione del registro degli pseudonimi dipende dalle scelte di ogni singola scuola, come l'ufficio didattica, il referente per l'inclusione, ecc. È fondamentale che il registro, solitamente organizzato in Word o Excel, **sia protetto da password e non venga mai stampato**, al fine di garantire la sicurezza e la riservatezza dei dati.

Come possono i docenti ricordare i codici degli pseudonimi?

In base alle scelte delle singole scuole, i codici degli pseudonimi vengono trasmessi ai docenti in modo sicuro. Ad esempio caricando i codice in un documento, **protetto da password**, nella Google Classroom o in Microsoft Teams.

Se il docente desidera raccogliere tutti i codici dei suoi studenti in un unico documento, si può utilizzare lo stesso metodo per ricordare le password: creare un documento protetto da password che contenga l'elenco dei nomi e dei cognomi degli studenti associati ai rispettivi codici pseudonimi. Questo documento mai va stampato

Nei verbali va sempre usato il codice degli pseudonimi?

No. Il codici degli pseudonimi va utilizzato solo quando si fa riferimento alla salute degli studenti (es. lo studente con codice 314 del registro della pseudonimizzazione, a seguito della prescrizione della nuova terapia farmacologica, ha migliorato il grado di attenzione durante le le lezioni). Ricorda! Se usi gli pseudonimi degli aluni non puoi scrivere nel verbale i nomi dei genitori. Nelle riunioni alla presenza dei genitori basterà indicare: madre presente/assente; padre presente/assente.

Quando non si fa riferimento alla salute va indicato il cognome e nome in chiaro, **come ad esempio nell'attribuzione dei voti agli scrutini**.

Come si possono organizzare in sicurezza i PDP e i PEI?

Durante la stesura dei PEI/PDP, che avviene tipicamente in modalità collettiva utilizzando Word o applicativi cloud, è obbligatorio:

1. **omettere il cognome e nome dello studente**, sostituendoli con il codice degli pseudonimi;
2. **omettere il cognome e nome dei genitori**, sostituendoli con la dicitura generica «I genitori:».

In questo modo, **i documenti risultano anonimi e possono essere memorizzati nel cloud, trasmessi tramite posta elettronica** o condivisi in altri modi, garantendo la protezione dei dati personali.

Come si firmano su carta i PDP e i PEI?

Una volta firmati dai genitori i PEI e i PDP **non sono più anonimi** quindi occorre porre in atto le seguenti misure di sicurezza:

- la firma autografa **leggibile** dei genitori deve essere apposta **presso gli uffici di segreteria**, che prenderanno immediatamente in custodia i documenti. Se la firma non è leggibile, è necessario aggiungere a mano il cognome e nome in stampatello.
- se, **con l'autorizzazione del dirigente Scolastico**, la firma dei genitori viene raccolta direttamente dal docente di sostegno o dal coordinatore di classe, questo assume la piena responsabilità della custodia e sicurezza dei documenti fino alla loro tempestiva consegna agli uffici di segreteria.

I documenti firmati non possono essere custoditi nei plessi.

Come si firmano elettronicamente i PDP e i PEI?

Nel caso di sottoscrizione con firma elettronica avanzata (FEA) del Ministro, è necessario seguire questi passaggi:

- il docente di sostegno o il coordinatore di classe trasmette per e-mail i documenti pseudonimizzati e privi del nome dei genitori alla segreteria della scuola;
- gli uffici di segreteria attivano il processo per la sottoscrizione tramite firma elettronica avanzata (FEA).

I docenti hanno accesso ai documenti contenenti i dati sulla salute degli studenti conservati nelle segreterie?

I documenti sia in formato cartaceo sia elettronico, che contengono dati relativi alla salute **riferibili direttamente o indirettamente agli studenti**, **devono essere conservati esclusivamente presso le segreterie scolastiche.**

Su richiesta del docente, anche per le vie brevi, di accedere ai documenti, il Dirigente Scolastico può:

- autorizzare i docenti a consultare i documenti presso gli uffici di segreteria (la raccolta degli eventuali appunti va riferita al codice degli pseudonimi, non alle iniziali dello studente);
- disporre che gli uffici di segreteria forniscano al docente richiedente una copia dei documenti adeguatamente anonimizzata.

I genitori possono fare fotografie o riprese video durante le manifestazioni scolastiche?

Non violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici.

Le immagini, in questi casi, **sono raccolte per fini personali e destinate a un ambito familiare o amicale** e non alla diffusione.

I genitori possono pubblicare solo le immagini/video dei loro figli. La pubblicazione di immagini/video di altre persone è possibile solo dopo averne ottenuto il consenso.

Gli studenti possono fare fotografie o riprese video durante le manifestazioni scolastiche come le visite didattiche ecc.?

Sì, le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale e non alla diffusione.

Gli studenti possono accordare il consenso al trattamento dei dati (compresa la diffusione delle immagini/video) **a partire da 14 anni.**

Gli alunni possono registrare le lezioni?

Sì. È lecito registrare la lezione **per scopi personali**, ad esempio per motivi di studio individuale, **compatibilmente con le specifiche disposizioni scolastiche al riguardo**.

https://www.garanteprivacy.it/home/faq/scuola-e-privacy

Non è invece ammessa la videoregistrazione della lezione in cui si manifestano le dinamiche di classe, neanche qualora si utilizzino piattaforme per la didattica a distanza.

(GPDP, "La scuola a prova di privacy", edizione 2023)

Il personale scolastico può pubblicare sui propri profili social personali le immagini degli studenti?

No, mai, la pubblicazioni di immagini/video di persone è **possibile solo dietro consenso di tutti gli interessati**.

Nel caso in cui le persone riprese **non siano riconoscibili** (es. volti pixellati o coperti con emoticon) non c'è trattamento di dati personali di conseguenza le immagini sono pubblicabili.

Quando è possibile la pubblicazione delle immagini degli studenti nei siti web della scuola?

Ci sono due i motivi per cui è possibile diffondere le immagini degli studenti:

1. la pubblicazione è **necessaria** per il perseguimento delle finalità didattiche di cui la scuola è portatrice (PTOF). In questo caso **non è necessaria la liberatoria**
2. la pubblicazione è **possibile**, su decisione del Dirigente Scolastico, per **promuovere** la scuola. In questo caso **è necessaria la liberatoria** (gli studenti con 14 anni compiuti possono dare direttamente il consenso).

Quando è possibile attivare una piattaforma didattica che profila gli studenti?

L'attivazione di una piattaforma didattica che profila gli studenti è possibile solo se sono soddisfatte **tre condizioni**:

1. 1'adozione della piattaforma è stata approvata dagli organi competenti come strumento necessario per il raggiungimento degli obiettivi didattici dell'offerta formativa;
2. tra la scuola e il fornitore della piattaforma è stato stipulato un contratto, **firmato dal Titolare del trattamento**, **in cui il fornitore si impegna a ricoprire il ruolo di Responsabile del trattamento dei dati**. Questo è quanto avviene, ad esempio, con il Registro Elettronico, Google Workspace e Microsoft 365;
3. se la piattaforma trasferisce i dati in paesi extra UE allora il trasferimento deve avvenire in maniera conforme al GDPR.

C'è un modo per poter utilizzare una piattaforma che non rispetti le tre condizioni?

La scuola non può attivare piattaforme che non rispettano il GDPR, e lo stesso vale per i docenti. Tuttavia, **le famiglie o gli studenti di almeno 14 anni possono iscriversi autonomamente alle piattaforme didattiche che ritengono più appropriate**.

Il docente, con l'autorizzazione del Dirigente Scolastico, potrebbe allora:

- informare le famiglie degli studenti con meno di 14 anni che tale piattaforma sarebbe utile per la didattica seppure non attivabile direttamente dalla scuola. I Genitori possono allora decidere di iscriversi alla piattaforma **con un indirizzo di posta personale** rapportandosi, ai fini della privacy, direttamente con il fornitore del servizio.
- chiedere agli studenti che hanno 14 anni compiuti di iscriversi in autonomia **con un loro indirizzo di posta personale**. Anche in questo caso è però una buona pratica informare i genitori che per motivi didattici il docente ha chiesto agli studenti di iscriversi alla piattaforma.

È possibile assegnare temi riguardanti il mondo familiare o personale degli alunni?

Sì. È possibile.
Nel momento in cui gli elaborati vengono letti in classe – specialmente se riguardano argomenti delicati – è affidata alla sensibilità di ciascun insegnante **la capacità di trovare il giusto equilibrio tra le esigenze didattiche e la tutela dei dati personali**.

Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente **riguardo al segreto d'ufficio e professionale**, nonché quelli relativi alla conservazione dei dati personali eventualmente contenuti nei temi degli alunni.

(GPDP, "La scuola a prova di privacy", edizione 2023)

È possibile correggere i compiti in classe a casa?

Sì, è possibile. In questo caso, **il docente è responsabile della custodia degli elaborati** e deve adottare tutte le misure di sicurezza necessarie per impedire l'accesso non autorizzato ai documenti.
Nelle griglie di valutazione eventualmente utilizzate **togliere qualsiasi riferimento a disabilità e DSA**

Buona pratica: chiedere agli studenti di sostituire il cognome e nome con il numero d'ordine del registro elettronico (alla riconsegna degli elaborati chiedere di mettere il cognome e nome)

I voti delle verifiche dei singoli studenti possono essere essere resi noti alla classe?

Se previsto o compatibile con i regolamenti di Istituto è possibile. La comunicazione dei voti scritti, orali e pratici dei singoli studenti alla classe, infatti, **non viola la privacy**.

Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti dei compiti in classe, delle interrogazioni o gli scrutini, né di consegnarli agli alunni in busta chiusa.

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1069385 **(documento web del 2004 confermato a pag. 72 GPDP, "La scuola a prova di Privacy, edizione 2023)**

Cosa occorre fare se un dipendente viene a conoscenza di un trattamento illecito dei dati?

Nel caso in cui il dipendente venga a conoscenza di una violazione dei dati personali 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, deve darne tempestiva notizia al Titolare del trattamento o al Responsabile della protezione dei dati.

Materiale utilizzabile per gli adempimenti di istruzione e formazione del personale di cui:

- **art 29 GDPR 2016/679**
- **art 32 c. 4 GDPR 2016/679**
- **art 39 c. 1, lett. b, GDPR 2016/679**
- **art 2 quaterdecies D. Lgs. 196/2003 ss.mm.ii**

Materiale destinato esclusivamente al personale scolastico dove il DPO è il dott. Pier Giorgio Galli
pggalli@gallilab.it - www.gallilab.it