SOS Dirigenti scolastici

Guide pratiche per affrontare i problemi quotidiani

IL DIRIGENTE E LA PRIVACY NELLE ISTITUZIONI SCOLASTICHE EUROPEE

GABRIELLA CHISARI

- Dal D.Lgs. 196/2003 al Regolamento europeo (GDPR)
- I Soggetti coinvolti nel trattamento dei dati
- Il GDPR: principi fondamentali
- I dati personali
- Trattamento dati nella scuola
- Il registro elettronico
- Casi comuni e campi di applicazione
- Normativa di riferimento

latecnicadellascuola

DAL D.LGS. N. 196/2003 AL REGOLAMENTO EUROPEO (GDPR)

Il **D.Lgs. n. 196 del 30/6/2003**, "Codice in materia di protezione dei dati personali", che ha superato e abrogato la precedente legge n. 675 del 31/12/1996, rappresenta la norma di riferimento primaria riguardo la privacy. Con tale decreto è stata introdotta la garanzia che il trattamento dei dati personali debba svolgersi nel rispetto del diritto e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Il decreto n. 196/2003 è stato integrato e modificato dal successivo **D.Lgs. n. 101 del 10/8/2018**, recante "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del **Regolamento (UE) 2016/679** del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, che ha abrogato la precedente direttiva 95/46/CE (Regolamento generale sulla protezione dei dati)".

Dal 25 maggio 2018, quindi, è divenuto pienamente applicabile in tutti gli Stati membri il suddetto Regolamento Ue 2016/679, noto come GDPR (General Data Protection Regulation) o RGPD (Regolamento Generale sulla Protezione dei Dati) che delinea le “Linee guida” in materia di protezione delle Persone Fisiche.

I SOGGETTI COINVOLTI NEL TRATTAMENTO DEI DATI

TITOLARE DEL TRATTAMENTO DEI DATI

Il Titolare del trattamento dei dati è la persona fisica, la persona giuridica, la Pubblica Amministrazione o qualsiasi altro ente a cui è consentito, singolarmente o insieme ad altri soggetti, di determinare le finalità e le modalità del trattamento dei dati personali (art. 4 GDPR). Qualora due o più soggetti si trovino ad agire contemporaneamente come titolare del trattamento, sono definiti contitolari.

L'intestazione della qualità di titolare del trattamento dei dati personali in capo all'istituzione scolastica implica che le attività connesse a tale ruolo (l'adozione di istruzioni e la vigilanza) debbano essere esercitate da chi è legittimato a manifestare la volontà dell'istituzione scolastica, ossia il Dirigente scolastico, il quale - in qualità di legale rappresentante - in concreto è chiamato a prendere decisioni sulle attività di trattamento da intraprendere e sulle modalità attraverso cui queste verranno svolte mediante il personale amministrativo e/o docente o le altre necessarie figure coinvolte.

Compiti del Titolare del trattamento dei dati

– individua il rischio connesso al trattamento e pone in sicurezza l'attività di trattamento dei dati
– rilascia l'informativa agli interessati
– attende all'esercizio dei diritti degli interessati
– nomina il Responsabile del trattamento dei dati e vigila sull'osservanza del suo contratto e dei suoi compiti
– compila il registro del trattamento dei dati
– nomina il Responsabile della Protezione dei dati (DPO/RPD)
– coopera con l'Autorità di controllo
– effettua la "valutazione d'impatto" (DPIA)
– accerta l'eventuale violazione dei dati personali (data breach), la documenta e la comunica al Garante.

RESPONSABILE DEL TRATTAMENTO DEI DATI

Il Responsabile del trattamento dei dati è la persona fisica, la persona giuridica, la Pubblica Amministrazione e qualsiasi altro ente preposto dal titolare al trattamento di dati personali. Ha il compito di mettere in atto misure tecniche e organizzative adeguate a soddisfare i requisiti richiesti dal GDPR e a garantire la tutela dei diritti dell'interessato.

Il responsabile è individuato tra i soggetti che per esperienza, capacità ed affidabilità forniscono idonea garanzia del pieno rispetto delle vigenti disposizioni in materia di trattamento, ivi compreso il profilo relativo alla sicurezza a tutela dei diritti degli interessati.

Ogni soggetto esterno, quale può essere un fornitore di servizi che prevede la gestione di dati personali (come ad esempio il registro elettronico), deve essere nominato come responsabile del trattamento. Occorre formalizzare con specifico incarico il rapporto tra titolare e responsabile, chiarendo gli obblighi e i limiti del trattamento dei dati e disciplinando l'incarico con un contratto o atto giuridico.

Al responsabile devono essere fornite, per iscritto, tutte le istruzioni in merito ai trattamenti da effettuare per conto del titolare, alle quali deve strettamente attenersi. Il responsabile deve inoltre assumersi responsabilità proprie, rispondendone, se del caso, alle autorità di controllo e alla magistratura.

Compiti del Responsabile del trattamento dei dati

– trattare dati soltanto su istruzione documentata del titolare del trattamento
– consentire i trattamenti solo a persone autorizzate con im-

pegno alla riservatezza o che abbiano un adeguato obbligo legale di riservatezza
– adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup)
– assistere il titolare per dare seguito alle richieste per l'esercizio dei diritti dell'interessato
– cancellare o restituire tutti i dati e cancellare le copie esistenti
– mettere a disposizione del titolare le informazioni per dimostrare il rispetto dei suddetti obblighi e consentire le ispezioni.

L'INCARICATO O AUTORIZZATO

L'incaricato o autorizzato è la persona fisica autorizzata dal titolare o dal responsabile a compiere operazioni di gestione e trattamento dei dati. A scuola lo sono gli assistenti amministrativi ma anche i docenti in quanto personale direttamente coinvolto nel processo formativo ed educativo. Essi operano sotto l'autorità diretta del titolare o del responsabile. Le persone autorizzate al trattamento dei dati personali non possono trattare tali dati se non sono istruite in tal senso dal titolare o dal responsabile.

Compiti dell'incaricato o autorizzato:

- svolgere i compiti assegnati secondo le istruzioni ricevute dal titolare del trattamento, operando nel pieno rispetto delle norme e delle misure di sicurezza
- collaborare con il titolare per verificare la conformità dei trattamenti
- adottare tutte le misure di sicurezza (es. cifratura; pseudonimizzazione; recupero da backup ecc.).

DESTINATARIO DEL TRATTAMENTO DEI DATI

Il Destinatario del trattamento dei dati è la persona fisica, la persona giuridica, la Pubblica Amministrazione o qualsiasi altro ente che riceve i dati personali dal titolare, necessari per eseguire i trattamenti per conto del titolare stesso o per conseguire proprie specifiche finalità.

- **Terzi:** sono tutti coloro che non sono identificati come titolari, responsabili o destinatari del trattamento.
- **Interessato:** è la persona fisica a cui si riferiscono i dati personali. Può esercitare i propri diritti, rivolgendosi direttamente al titolare del trattamento.
- Il **DPO** (Data Protection Officer) o RPD

IL RESPONSABILE PER LA PROTEZIONE DEI DATI

Il Responsabile per la Protezione dei Dati (Data Protection Officer, indicato anche con l'acronimo italiano RPD) è una figura introdotta dal GDPR, che deve possedere una buona padronanza dei processi informatici, della sicurezza dei dati (inclusa la gestione dei cyber-attacchi) e di altre questioni riguardanti il mantenimento e l'elaborazione di dati personali e sensibili. La sua responsabilità principale è quella di osservare, valutare e organizzare la gestione del trattamento di dati personali (e dunque la loro protezione) all'interno di un'azienda (sia essa pubblica che privata), affinché questi siano trattati nel rispetto delle normative, in tema di privacy, europee e nazionali.

Compiti del Responsabile per la Protezione dei Dati

- assiste il titolare/responsabile nel controllo del rispetto a livello interno del Regolamento
- è un consulente del titolare/responsabile
- svolge funzioni di controllo sui trattamenti
- è generalmente una **figura esterna** alla scuola
- il Responsabile per la protezione dei dati (art. 37 GDPR), quindi, è individuato in funzione delle qualità professionali e scelto per la conoscenza specialistica della normativa in materia di

dati personali; è tenuto a verificare l'osservanza delle norme del Regolamento da parte del titolare e nel caso di valutazioni di impatto, se richiesto dal titolare, è tenuto a consultarsi con esso.

IL GDPR: PRINCIPI FONDAMENTALI

Di seguito si indicano i principali aspetti e contenuti introdotti dal GDPR.

– **Responsabilizzazione o Accountability** del Titolare del trattamento, il quale ha il compito di assicurare ed essere in grado di comprovare il rispetto dei principi fondamentali applicabili al trattamento dei dati personali (art. 5) che devono essere:
  • trattati secondo "liceità, correttezza e trasparenza"
  • raccolti per "finalità determinate, esplicite e legittime"
  • adeguati, pertinenti e limitati rispetto alle finalità
  • esatti
  • limitati nella conservazione
  • trattati garantendo sicurezza e integrità.

– Principi di "**privacy by design**" e "**privacy by default**" e precisamente:
  • ai sensi dell'articolo 25, paragrafo 1, del GDPR per privacy by design si intende l'obbligo per il titolare, di mettere

in atto "misure tecniche e organizzative adeguate, quali la pseudonimizzazione, (procedimento che impedisce di identificare direttamente la persona cui si riferisce il dato, in quanto tali dati non possono essere attribuiti a un individuo specifico senza l'uso di ulteriori informazioni) e la minimizzazione (che richiede che i titolari dei dati personali raccolgano solo le informazioni necessarie al raggiungimento delle finalità del trattamento stesso, utilizzando e conservando solamente i dati che sono realmente indispensabili per uno scopo definito) e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del regolamento e tutelare i diritti degli interessati".

- Ai sensi dell'articolo 25, paragrafo 2, del GDPR, per privacy by default si intende che "Il titolare del trattamento metta in atto misure tecniche e organizzative adeguate per garantire che siano trattati, **per impostazione predefinita**, solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In particolare,

dette misure garantiscono che, per impostazione predefinita, non siano resi accessibili dati personali a un numero indefinito di persone fisiche senza l'intervento della persona fisica". In sostanza, per impostazione predefinita, devono essere trattati esclusivamente i dati personali necessari per la **specifica finalità del trattamento** e per il periodo strettamente necessario, garantendo inoltre la non eccessività di tutti i dati raccolti.

– Concetto di **rischio e adeguatezza delle misure di sicurezza** e di data breach ovvero di "una violazione di sicurezza - accidentale o in modo illecito - che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati". Secondo il GDPR, la notifica di eventuali violazioni di dati deve avvenire possibilmente senza ingiustificato ritardo e, ove possibile, entro 72 ore, dal momento in cui si è venuto a conoscenza della violazione, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. L'eventuale ritardo dovrà essere motivato.

I rischi insiti nel trattamento dei dati riguardano la **distruzione, perdita, modifica, divulgazione, accesso non autorizzato** che mettono in pericolo la sicurezza sulla protezione dei dati personali, fondata sui criteri di riservatezza, integrità e disponibilità.

Le cause di violazione possono essere individuate in tre tipologie:

1. **comportamenti errati** (disattenzione, inconsapevolezza, condotte fraudolente, furto, smarrimento) da parte del personale amministrativo scolastico, dei docenti, degli alunni o dei genitori
2. **violazione informatica** (virus, malware, sabotaggio, obsolescenza della strumentazione, degrado, malfunzionamento) esterna e/o interna
3. **violazione contestuale** (eventi imprevedibili naturali, dolosi, artificiali o accidentali) all'impianto scolastico.

– **Sanzioni amministrative pecuniarie**: esse vengono applicate in caso di violazione dei dati e variano a seconda delle disposizioni violate; sono applicate sulla base di criteri che devono tenere in conto:

- della natura, della gravità e della durata della violazione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito, ma anche il carattere doloso o colposo della violazione
- delle misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati e il loro grado di responsabilità, tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 25 (by design/by default) e 32 (misure sicurezza)
- delle categorie di dati personali interessate dalla violazione
- di eventuali precedenti violazioni commesse dal titolare del trattamento o dal responsabile del trattamento e il grado di cooperazione con l'autorità di controllo al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi
- della maniera in cui l'autorità di controllo ha preso conoscenza della violazione, in particolare se, e in che misura,il titolare del trattamento o il responsabile del trattamento ha notificato la violazione (data breach)
- di eventuali altri fattori aggravanti o attenuanti applicabili

alle circostanze del caso, ad esempio i benefici finanziari conseguiti o le perdite evitate, direttamente o indirettamente, quale conseguenza della violazione.

– Procedura di **valutazione d'impatto** sulla protezione dei dati (DPIA) finalizzata a descrivere il trattamento, valutarne necessità e proporzionalità e facilitare la gestione dei rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento dei loro dati personali. Essa è obbligatoria per trattamenti che prevedono l'uso di nuove tecnologie.

– Nomina obbligatoria di un **Responsabile della protezione dei dati** (RPD).

– Regole più chiare su **informativa e consenso**. In particolare deve essere resa un'informativa chiara e puntuale quale strumento di trasparenza riguardo al trattamento dei dati personali e all'esercizio dei diritti. Il consenso dell'interessato al trattamento dei dati personali deve essere preventivo e inequivocabile, anche quando espresso attraverso mezzi elettronici (ad esempio, selezionando un'apposita

casella in un sito web). Per trattare i dati sensibili, il Regolamento prevede che il consenso deve essere anche «esplicito». Viene esclusa ogni forma di consenso tacito (il silenzio, cioè, non equivale al consenso) oppure ottenuto proponendo a un interessato una serie di opzioni già selezionate. Il consenso potrà essere revocato in ogni momento.

– Criteri rigorosi per il **trasferimento dei dati al di fuori dell'Ue**: Resta vietato il trasferimento di dati personali verso Paesi situati al di fuori dell'Unione europea o organizzazioni internazionali che non rispondono agli standard di adeguatezza in materia di tutela dei dati, rispetto ai quali il Regolamento introduce criteri di valutazione più stringenti.

I DATI PERSONALI

Secondo la Commissione Europea "i **dati personali** sono qualunque informazione relativa a un individuo, collegata alla sua vita sia privata, sia professionale o pubblica", che identificano o rendono identificabile, direttamente o indirettamente, una persona fisica e che possono fornire informazioni sulle sue caratteristiche, le sue abitudini, il suo stile di vita, le sue relazioni personali, il suo stato di salute, la sua situazione economica, ecc.

Particolarmente importanti sono i **dati che permettono l'identificazione diretta** - come i dati anagrafici (ad esempio: nome e cognome), le immagini, ecc. - e i **dati che permettono l'identificazione indiretta**, come un numero di identificazione (ad esempio, il codice fiscale, l'indirizzo IP, il numero di targa).

Molta attenzione va prestata al trattamento dei dati sensibili, cioè a quei dati personali idonei a rivelare:

- l'origine razziale ed etnica
- le convinzioni religiose, filosofiche o di altro genere
- i dati personali idonei a rivelare lo stato di salute e la vita sessuale

– le opinioni politiche, l'adesione a partiti, sindacati, associazioni od organizzazioni a carattere religioso, filosofico, politico o sindacale
– i dati personali relativi a condanne penali o reati
– i dati biometrici.

La scuola è il luogo dove vengono trattati molti dati personali e perlopiù di minori. Di conseguenza sono necessarie una particolare responsabilità e grande attenzione da parte del Dirigente scolastico, che, in quanto rappresentante legale dell'Istituto scolastico, è titolare del trattamento dei dati, e deve quindi agire nel rispetto e nell'applicazione di tutte le norme e di quanto il Garante stabilisce e indica attraverso l'individuazione di norme, emanazione di provvedimenti, proposte di linee guida e pareri. Tra i dati sensibili più comuni gestiti nella scuola si pongono, per esempio a fianco dei dati anagrafici, quelli relativi alla salute e specificatamente nei seguenti casi:

– gestione delle assenze per malattia
– insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie
– partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione

– regime alimentare differenziato dovuto a intolleranze, allergie o specifiche patologie.

A tal proposito, si segnala che non è consentito pubblicare online una circolare contenente:

– i nomi degli studenti con disabilità o con DSA, (neanche indicando le sole iniziali)
– i nomi degli alunni che seguono un regime alimentare differenziato per motivi di salute.

TRATTAMENTO DATI NELLA SCUOLA

- **Area della Didattica**, che tratta tutti i dati relativi agli alunni attraverso il fascicolo personale (curriculum studi, dati personali, dati dei genitori) e i registri di iscrizione, tasse scolastiche, certificati, diplomi).
- **Area del Personale**, che gestisce tutti i dati del personale docente e ATA riferiti al rapporto di lavoro (dati personali, dei familiari, relativi al servizio prestato, alle assenze, al curricolo studi, all'aggiornamento e formazione, ai procedimenti disciplinari o di valutazione…).
- **Area della Contabilità** che tratta i pagamenti, i rapporti con i fornitori e i loro dati.
- **Area degli Affari generali** attraverso il protocollo, gli archivi, i rapporti con enti e imprese.

Secondo quanto stabilito dal GDPR, tutti i dati personali devono essere:

- **trattati in modo lecito, corretto e trasparente** nei confronti dell'interessato senza rischiare di essere fraintendibili
- **raccolti per un determinato fine e in maniera esplicita**. Non

possono dunque essere usati per scopi diversi da quello iniziale, ad eccezione di ricerca scientifica, storica o fini statistici

– **raccolti** se trovano fondamento in una idonea base giuridica (consenso, legittimi interessi, ecc.)
– **adeguati, pertinenti e minimizzati** al necessario
– **esatti, aggiornati** costantemente e **rettificati o cancellati** se inesatti
– **conservati limitatamente** al tempo necessario al conseguimento delle finalità per le quali sono trattati e non più, ad eccezione di archiviazione nel pubblico interesse, di ricerca scientifica, storica o fini statistici
– **trattati in maniera adeguata** garantendo sicurezza e protezione da trattamenti non autorizzati o illeciti, da perdita, distruzione o danno accidentale attraverso misure tecniche e organizzative adeguate. A tal fine occorre tenere e aggiornare il registro dei trattamenti effettuati, da fornire alle autorità in caso di controllo.

L'istituzione scolastica pertanto può trattare qualunque dato, purché sia lecito, rientri tra le sue finalità, sia circoscritto nel tempo, secondo le perimetrazioni che rimandano ai prin-

cipi della liceità, della limitazione e della minimizzazione. Quest'ultimo principio richiama infatti la situazione in cui i "dati devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità del trattamento (art. 5 GDPR 2016/79).

IL REGISTRO ELETTRONICO

Particolare attenzione va prestata all'uso del registro elettronico dove sono veicolati i dati personali degli alunni.
Recentemente il Garante Privacy ha emanato la deliberazione del 19 dicembre 2024, avente ad oggetto "Attività ispettiva curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio/giugno 2025", includendo, tra le aree di intervento del piano ispettivo 2025, le verifiche sul trattamento dei dati effettuato attraverso i registri elettronici.
L'obiettivo di queste ispezioni è verificare la conformità al GDPR e alle altre normative in materia di protezione dei dati personali nel contesto specifico dell'utilizzo dei registri elettronici.
In particolare le ispezioni saranno indirizzate ai seguenti aspetti:

– le misure di sicurezza adottate per proteggere i dati contenuti nei registri elettronici da accessi non autorizzati, perdita o furto
– le modalità di gestione degli accessi al registro elettronico

da parte del personale scolastico, degli studenti e dei genitori
– l'informativa fornita agli interessati (studenti e genitori) in merito al trattamento dei loro dati personali attraverso il registro elettronico
– la nomina dei responsabili del trattamento e degli incaricati, nonché la definizione dei ruoli e delle responsabilità
– la gestione dei consensi, se necessari, per particolari trattamenti di dati (es. pubblicazione di foto o video degli studenti)
– il rispetto dei principi di minimizzazione e proporzionalità nel trattamento dei dati, evitando la raccolta di informazioni non necessarie
– le modalità di conservazione e cancellazione dei dati contenuti nei registri elettronici.

In tale situazione, per prevenire rischi e violazione dei dati e non incorrere nelle previste sanzioni, si suggerisce che il Dirigente scolastico, in qualità di titolare del trattamento, ponga massima attenzione e metta in atto le seguenti azioni preventive:

– aggiornare le misure di sicurezza tecniche e organizzative per garantire un livello adeguato di protezione dei dati anche in collaborazione con il DPO

- effettuare un'analisi approfondita dei rischi relativi al trattamento dei dati attraverso i registri elettronici
- verificare che le informative fornite agli interessati siano conformi
- formare e sensibilizzare il personale scolastico in merito alle normative sulla protezione dei dati e alle corrette modalità di utilizzo dei registri elettronici
- documentare tutte le attività svolte in materia di protezione dei dati, al fine di dimostrare il rispetto e la conformità alla normativa
- rafforzare i controlli e i rapporti con i fornitori di servizi esterni per evitare violazioni.

Si ricorda, altresì, che con la recente nota n. 2773 del 4/4/2025 il Ministero ha dato indicazioni specifiche alle istituzioni scolastiche sulle modalità di **gestione dei registri on line**; in particolare ha evidenziato come il **registro elettronico** debba essere destinato:

- alla gestione delle attività didattiche da parte dei docenti
- alla trasmissione delle comunicazioni istituzionali da parte del Ministero e delle Istituzioni alle famiglie, alle studentesse e agli studenti

– alla presa visione dell'attività scolastica svolta dalle studentesse e dagli studenti da parte delle famiglie.

È stato inoltre sottolineato come il registro **non debba essere destinato a servizi commerciali o ad attività non riconducibili alle finalità sopra evidenziate**.

Viene esclusa anche la possibilità di trasferire dati a soggetti terzi, salvo che ciò sia strettamente connesso al funzionamento del Registro.

La circolare riporta in allegato una serie di istruzioni e indicazioni riguardanti le modalità di "identificazione e di autenticazione, di integrazione, di interoperabilità, di data-protection, di sicurezza dei dati e di trasferibilità dei dati contenuti nel Registro". Ciò a sottolineare la delicatezza dell'utilizzo corretto del registro elettronico, "essendo strettamente connesso all'espletamento di funzioni pubbliche essenziali proprie delle Istituzioni Scolastiche, con conseguente coinvolgimento di molteplici dati personali di studentesse e studenti, genitori, dirigenti scolastici e personale scolastico, come anche precisato dal Garante per la Protezione dei Dati Personali all'interno del Vademecum «La scuola a prova di privacy», Ed. 2023".

> VAI ALLA NOTA MIM n. 2773 del 4/4/2025

CASI COMUNI E CAMPI DI APPLICAZIONE

Considerato il vastissimo campo di applicazione delle norme sulla privacy nella scuola il Garante per la Protezione dei Dati Personali (GPDP) ha pubblicato già nel 2016 un documento di indirizzo "**La scuola a prova di privacy**", aggiornato con l'edizione 2023, alla luce del nuovo contesto formativo determinato soprattutto dall'innovazione tecnologica degli ultimi anni. Si pensi al costante uso del web da parte degli studenti, al registro elettronico, alla messaggistica, ai social media, ai tablet. Con tale documento il Garante ha fornito alcune indicazioni e chiarimenti relativi a diversi casi specifici e molto frequenti a scuola per aiutare i giovani, il personale della scuola e i genitori a tutelarsi di fronte ai continui rischi connessi allo sviluppo del mondo digitale.

Di seguito alcuni casi tra i più comuni:

– **voti ed esami**: pur nel rispetto della trasparenza degli atti, gli esiti degli scrutini non possono essere pubblicati on line, in quanto la pubblicazione costituirebbe una forma di diffusione di dati non conforme all'attuale quadro normati-

vo in materia di protezione dei dati. Infatti i voti pubblicati online rimarrebbero in rete e potrebbero essere utilizzati da soggetti estranei alla scuola, violando in tal modo la riservatezza degli studenti, perlopiù minori. Di conseguenza gli esiti degli scrutini delle classi intermedie delle scuole secondarie di primo e di secondo grado e di ammissione agli esami di Stato del secondo ciclo di istruzione vanno resi disponibili, con la sola indicazione "ammesso" e "non ammesso" alla classe successiva, nell'area riservata del registro elettronico cui possono accedere solo gli studenti della classe di riferimento.

I voti riportati nelle singole discipline dall'alunno, invece, vanno resi disponibili nell'area riservata del registro elettronico a cui può accedere esclusivamente, con le proprie credenziali, il singolo studente o la propria famiglia.

Solo nel caso in cui la scuola non utilizzi il registro elettronico è possibile affiggere all'interno dell'istituto i tabelloni con i voti ma senza fornire altri dati sugli studenti (condizioni di salute, DSA/BES, alunni portatori di handicap, prove differenziate, altro).

– **Circolari e comunicazioni**: Non è consentito inserire nelle circolari o nelle comunicazioni scolastiche dati personali che rendano identificabili gli alunni coinvolti in particolari situazioni, come, per esempio, per i casi di bullismo o per provvedimenti disciplinari, o dove si faccia riferimento a dati sulla salute; si pensi alle convocazioni di genitori, docenti e operatori sanitari per la predisposizione del PEI contenenti gli elenchi di alunni con disabilità o a circolari con i dati di alunni con DSA, anche indicati con le sole iniziali. Non è ammessa neanche la pubblicazione sul sito web di elenchi relativi alla composizione delle classi. I nominativi degli studenti distinti per classe vanno eventualmente comunicati alla email fornita dalla famiglia in fase di iscrizione.
– **Cellulari e tablet**: l'uso di cellulari e smartphone è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta comunque agli istituti scolastici decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari o altri strumenti elettronici in aula, anche alla luce della Nota ministeriale n. 5274 dell'11 luglio 2024, che

ha disposto il divieto di utilizzo in classe del telefono cellulare, anche a fini educativi e didattici, per gli alunni dalla scuola d'infanzia fino alla secondaria di primo grado. Inoltre, non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. E' bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie o perfino in veri e propri reati. Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line. Non è ammessa invece la videoregistrazione della lezione in cui si manifestano le dinamiche di classe. Naturalmente va garantito agli studenti con DSA o altre specifiche patologie l'utilizzo di strumenti (registratore, computer, tablet, smartphone) quale utili dispositivi per l'apprendimento.

– **Recite e gite 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 a fini personali e destinati ad un ambito familiare o amicale; nel caso in cui si intenda pubblicarle o diffonder-

le in rete, anche sui social network, è necessario ottenere il consenso delle persone presenti nei video o nelle foto. Risulta pertanto opportuno fare questa comunicazione, in forma ufficiale, ai genitori al fine di sollevare la scuola da qualsiasi responsabilità.

– **Questionari per attività di ricerca**: L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori, nel caso di minori, siano stati prima informati sugli scopi delle ricerca, le modalità del trattamento e le misure di sicurezza adottate. Gli studenti e i genitori devono essere lasciati liberi di non aderire alle iniziative.
– **Graduatorie del personale e supplenze**: Le scuole possono pubblicare sui propri siti istituzionali le graduatorie di docenti e personale ATA indicando solamente i dati strettamente necessari come nome e cognome, punteggio e posizione in graduatorie; non vanno riportati dati non pertinenti quali numeri di telefono o indirizzi.

Alla luce di quanto sopra definito, gli istituti scolastici devono sempre vigilare sulle diverse situazioni occorrenti e devono rendere noto - attraverso un'adeguata **informativa** con le

modalità ritenute più opportune, eventualmente anche online - quali dati raccolgono, come li utilizzano e a quale fine, ponendo estrema cautela nel trattare i dati di studenti e personale, in conformità al regolamento sul trattamento dati.
Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

NORMATIVA DI RIFERIMENTO

- Regolamento europeo n. 679 del 27/4/2016 del Garante per la Protezione dei Dati Personali (GDPR)
  > VAI AL REGOLAMENTO

- D.Lgs. n. 101 del 10/8/2018, Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del Regolamento (UE) 679/2016 del Parlamento europeo e del Consiglio, del 27/4/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali
  > VAI ALLA NORMA

- D.Lgs. n. 196 del 30/6/2003 - Codice in materia di protezione dei dati personali
  > VAI ALLA NORMA

- Linee guida cookie e altri strumenti di tracciamento del 10 giugno 2021 del Garante per la Protezione dei Dati Personali (GDPR), aggiornato con il vademecum "La scuola a prova di privacy" del 2023
  > VAI ALLE LINEE GUIDA COOKIE
  > VAI AL VADEMECUM "LA SCUOLA A PROVA DI PRIVACY"

- Delibera del 19/12/2024 - Attività ispettiva curata dall'Ufficio del Garante, anche per mezzo della Guardia di finanza, limitatamente al periodo gennaio/giugno 2025
  > VAI ALLA NORMA

– Nota MIM n. 2773 del 4/4/2025 - Indicazioni in merito alle modalità di gestione del registro elettronico
> VAI ALLA NORMA