Ministero
Istruzione
Università
Ricerca

GEMINI
STUDIO PRIVACY

PRIVACY e SCUOLA

Articolo 16, paragrafo 1, del trattato sul funzionamento dell'Unione europea (TFUE):

"Ogni Persona ha diritto alla protezione dei dati personali che la riguardano"

Privacy e Scuola
www.studioprivacy.eu

QUADRO NORMATIVO

- Direttiva Europea 95/46/CE
- Legge 675 del 31 dicembre 1996
- D.Lgs 196 del 30 giugno 2003
- DM 305/2006
- Nuovo Regolamento Europeo 2016/679/CE
- D.Lgs 101 del 10/08/2018

Cos'è la Privacy?

Tutelare la Privacy significa tutelare la **riservatezza dell'individuo**. **La Privacy è riconosciuta come un diritto fondamentale dell'uomo direttamente collegato alla tutela della dignità umana**.
In particolare la privacy può essere considerata come una linea di demarcazione tra i poteri di intrusione della società e la sfera privata dell'uomo.

I dati personali devono essere:

- trattati in modo lecito e corretto;
- raccolti e registrati per scopi determinati, espliciti e **legittimi**;
- esatti e, se necessario, aggiornati;
- pertinenti, completi e **non eccedenti** rispetto alle finalità per le quali sono stati raccolti o successivamente trattati;
- **conservati** per un periodo di tempo non superiore a quello necessario agli scopi per cui sono stati raccolti o trattati.

Chi è obbligato a rispettare la Privacy?

Il soggetto (azienda privata, pubblica amministrazione, libero professionista) che per qualsiasi motivo raccoglie dati personali, è obbligato a rispettare le norme sulla privacy.
Non ricade nell'ambito di applicazione della legge solo il trattamento di dati personali effettuato da persone fisiche per fini esclusivamente personali (agende personali, rubriche, raccolte di foto).

Adempimenti minimi

Adempimenti Minimi

Gli adempimenti per l'adeguamento a quanto stabilito dalla normativa Privacy sono relativi essenzialmente a 4 ambiti:

1) DATI E TRATTAMENTI: individuazione delle tipologie di dati trattati e delle finalità e modalità del trattamento. Per "trattamento dei dati si intende qualunque operazione, svolta con o senza l'ausilio di strumenti elettronici, concernenti le attività di raccolta, registrazione, organizzazione, conservazione, consultazione, elaborazione, blocco, modificazione, utilizzo, interconnessione, comunicazione, diffusione, cancellazione, distruzione, selezione, estrazione, raffronto dei dati.

2) SOGGETTI: individuazione dei soggetti che effettuano il trattamento dei dati (titolare, delegato, incaricati, responsabili esterni) e loro nomina e formazione.

3) TUTELA DEGLI INTERESSATI: informativa ai soggetti i cui dati si vogliono raccogliere. Raccolta del consenso degli interessati. Garanzia del diritto di accesso per gli interessati.

4) SICUREZZA: adozione di misure di sicurezza fisiche e tecnologiche per la tutela dei dati personali.

I DATI PERSONALI

Il GDPR 2016/679 all'art. 4 prevede la seguente definizione di Dato Personale e la sua conseguente classificazione:

Dato personale: qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»). Si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, i dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale. I dati personali si classificano in:

Dati genetici: i dati personali relativi alle caratteristiche genetiche ereditarie o acquisite di una persona che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica, e che risultano in particolare dall'analisi di un campione biologico del soggetto in questione;

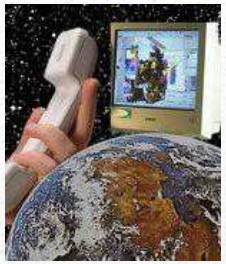
Dati biometrici: i dati personali, ottenuti da un trattamento tecnico specifico, relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici;

Dati relativi alla salute: i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute.

All'artt. 9 e 10 classifica alcuni dati di "tipo particolare":

Categorie particolari di tipi di dati: dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici e i dati biometrici intesi a identificare in modo univoco una persona fisica; dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. Dati personali relativi alle condanne penali e ai reati o connessi a misure di sicurezza.

COMUNICAZIONE



DIFFUSIONE

Dare conoscenza dei dati personali a uno o più soggetti **DETERMINATI** diversi dall'interessato in qualunque forma anche mediante la loro messa in disposizione o consultazione

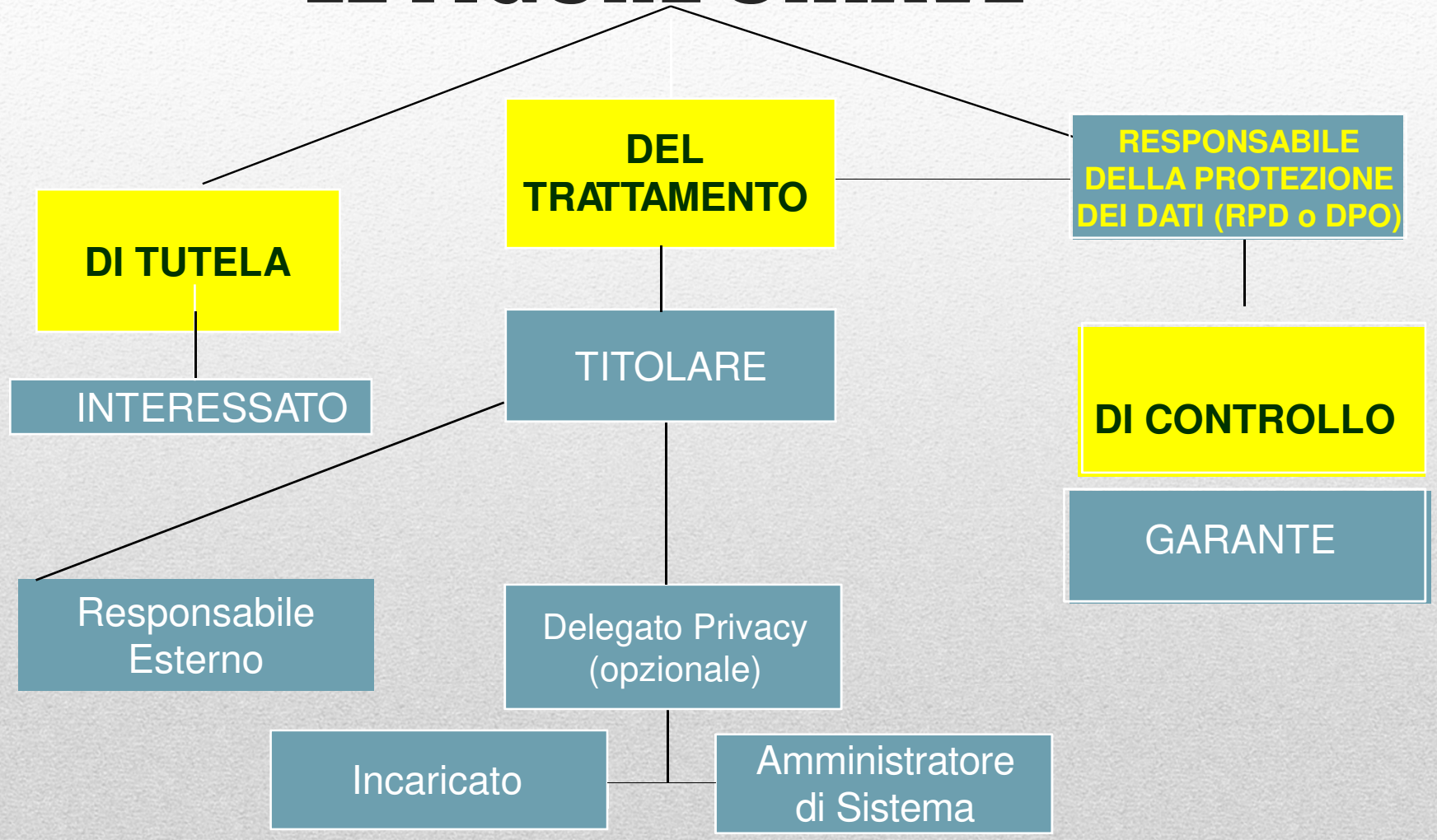
Dare conoscenza dei dati a soggetti **INDETERMINATI** in qualunque forma anche mediante la loro messa in disposizione o consultazione

Occorre il consenso specifico dell'interessato

Per alcuni trattamenti è vietata la diffusione

(ad esempio tutti i dati personali trattati dalle pubbliche amministrazioni, in mancanza di una Legge o di un Regolamento che lo permetta)

LE FIGURE CHIAVE



IL SISTEMA di GESTIONE PRIVACY

PROCEDURALI	DOCUMENTALI	FISICO/LOGICHE
Insieme di Procedure organizzative Istituzionali riguardanti le aree: Didattica, Personale ATA e Docenti, ICT, Sanità, Rapporti Scuola/Famiglia, ecc.	Insieme delle evidenze documentali che mirano ad una corretta informazione delle Policy interne, alla legittimità del trattamento, alle nomine interne ed esterne, all'obbligatoria Formazione, all'evidenza del funzionamento del Sistema di Gestione Privacy	Misure poste a protezione delle sedi aziendali, alla gestione ed archiviazione dei documenti, alla gestione della Sicurezza IT, alla salvaguardia dei dati in generale.

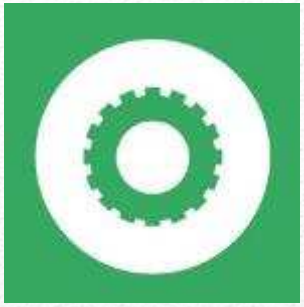
SGP: STATO DELL'ARTE

IERI	OGGI	DOMANI
DRSP NOMINA INCARICATI INFORMATIVE MISURE MINIME IT	PROFILI RESP.TA' AGG. NOMINE DETTAGLIATE ADS ISTRUZIONI CORRETTE INFORMATIVE e CONSENSI AMPLIATI REGOL. USO SISTEMI INFORMATIVI REGOL. PERSONALE EMAIL E INTERNET	**IMPLEMENTAZIONE DI UN SISTEMA PRIVACY** IMPIANTO DOCUMENTALE E ORGANIZZATIVO; EVIDENZE DELLA CORRETTA APPLICAZIONE DELLE NORME; MISURE TECNICHE ADEGUATE

GDPR

Principi fondamentali

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 e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)



Fondamenti di liceità del trattamento

Il regolamento conferma che ogni trattamento **deve trovare fondamento in un'idonea base giuridica**. I fondamenti di liceità del trattamento sono **il consenso**, l'adempimento di obblighi contrattuali, gli interessi vitali della persona interessata o di terzi, **gli obblighi di legge cui è soggetto il titolare**, **l'interesse pubblico o esercizio di pubblici poteri**, l'interesse legittimo prevalente del titolare o di terzi cui i dati vengono comunicati.

L'Informativa

I contenuti dell'informativa sono più ampi rispetto al Codice. In particolare, la Pubblica Amministrazione deve sempre specificare i dati di contatto del DPO (Data Protection Officer), reso obbligatorio con l'avvento del GDPR.

Ove esistente, la base giuridica del trattamento, qual è il suo interesse legittimo se quest'ultimo costituisce la base giuridica del trattamento, nonché se trasferisce i dati personali in Paesi terzi e, in caso affermativo, attraverso quali strumenti.

Il titolare deve specificare il periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione, e il diritto di presentare un reclamo all'autorità di controllo.

Modalita' per l'esercizio dei diritti

Il termine per la risposta all'interessato è, per tutti i diritti (compreso il diritto di accesso) entro 1 mese, estendibile fino a 3 mesi in casi di particolare complessità; il titolare deve comunque dare un riscontro all'interessato entro 1 mese dalla richiesta, anche in caso di diniego.

Il Titolare ha il diritto di richiedere informazioni necessarie ad identificare l'interessato, e quest'ultimo ha il dovere di fornirle secondo modalità idonee.

Spetta al titolare valutare la complessità del riscontro all'interessato e stabilire l'ammontare dell'eventuale contributo da chiedere all'interessato, ma soltanto se si tratta di richieste manifestamente infondate o eccessive (anche ripetitive), ovvero se sono chieste più "copie" dei dati personali nel caso del diritto di accesso; in quest'ultimo caso il titolare deve tenere conto dei costi amministrativi sostenuti. Il riscontro all'interessato di regola deve avvenire in forma scritta anche attraverso strumenti elettronici che ne favoriscano l'accessibilità; può essere dato oralmente solo se così richiede l'interessato stesso.

La risposta fornita all'interessato deve essere concisa, trasparente e facilmente accessibile, oltre a utilizzare un linguaggio semplice e chiaro.

ACCOUNTABILITY: IL PRINCIPIO DI 'RESPONSABILIZZAZIONE'

Il regolamento pone con forza l'accento sulla "responsabilizzazione", ossia sull' adozione di comportamenti preventivi tali da dimostrare la concreta adozione di misure finalizzate ad assicurare l'applicazione del regolamento.

Tali criteri sono sintetizzato dalle espressioni "by design" e "by default", ossia dalla necessità di valutare il trattamento prevedendo, fin dall'inizio, le garanzie indispensabili al fine di soddisfare i requisiti di tutela dei dati degli interessati, tenendo conto del contesto e dei rischi relativi. Tutto questo deve avvenire ex ante, cioè prima di procedere al trattamento dei dati ed i titolari devono, di conseguenza, prevedere delle attività specifiche e dimostrabili. Dunque, l'intervento delle autorità di controllo sarà principalmente "ex post", ossia si collocherà successivamente alle determinazioni assunte autonomamente dal titolare.

Registro dei trattamenti

Tutti i titolari e i responsabili di trattamento, eccettuati gli organismi con meno di 250 dipendenti, ma solo se non effettuano trattamenti a rischio, devono tenere un registro delle operazioni di trattamento. Si tratta di uno strumento fondamentale non soltanto ai fini dell'eventuale supervisione da parte del Garante, ma anche allo scopo di disporre di un quadro aggiornato dei trattamenti in essere all'interno di un soggetto pubblico indispensabile per ogni valutazione e analisi del rischio. Il registro deve avere forma scritta, anche elettronica, e deve essere esibito su richiesta al Garante.

Raccomandazioni:

La tenuta del registro dei trattamenti non costituisce un adempimento formale bensì parte integrante di un sistema di corretta gestione dei dati personali.

MISURE DI SICUREZZA E DATA BREACH

Le misure di sicurezza devono garantire un livello di sicurezza adeguato al rischio del trattamento.

Tutti i titolari dovranno notificare all'Autorità di controllo le violazioni di dati personali ("Data Breach"), di cui vengano a conoscenza, entro 72 ore e comunque "senza ingiustificato ritardo", ma soltanto se ritengono probabile che da tale violazione derivino rischi per i diritti e le libertà degli interessati.

Pertanto la notifica all'Autorità dell'avvenuta violazione non è obbligatoria, essendo subordinata alla valutazione del rischio per gli interessati, che spetta, ancora una volta, al titolare. Se la probabilità di tale rischio è elevata, si dovrà informare delle violazione anche gli interessati, sempre "senza ingiustificato ritardo";

MISURE DI SICUREZZA E DATA BREACH

Non è richiesta la comunicazione all'interessato se è soddisfatta una delle seguenti condizioni:

a) il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione (es. cifratura dei dati)

b) il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato

c) detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica.

Tutti i titolari di trattamento dovranno in ogni caso documentare le violazioni di dati personali subite, nonché le relative circostanze e conseguenze e i provvedimenti adottati

Responsabile della protezione dei dati (DPO)

Il Responsabile della protezione dei dati, nominato dal titolare del trattamento, dovrà:

1. possedere un'adeguata conoscenza della normativa e delle prassi di gestione dei dati personali, anche in termini di misure tecniche e organizzative o di misure atte a garantire la sicurezza dei dati. Non sono richieste attestazioni formali o l'iscrizione ad appositi albi professionali, anche se la partecipazione a master e corsi di studio/professionali può rappresentare un utile strumento per valutare il possesso di un livello adeguato di conoscenze.
2. adempiere alle sue funzioni in piena indipendenza e in assenza di conflitti di interesse.
3. operare alle dipendenze del Titolare del trattamento oppure sulla base di un contratto di servizio.

Il titolare del trattamento dovrà mettere a disposizione del Responsabile della protezione dei dati le risorse umane e finanziarie necessarie all'adempimento dei suoi compiti.

La figura del DPO è OBBLIGATORIA per tutti gli Enti Pubblici e doveva essere nominata entro e non oltre il 24/05/2018.

DPO: Compiti e attività

- informare e consigliare in merito agli obblighi derivanti dalla normativa in vigore e conservare la documentazione relativa a tale attività e alle risposte ricevute;
- sorvegliare l'attuazione e l'applicazione sia della normativa in vigore che delle politiche Privacy, compresi l'attribuzione delle responsabilità e la formazione del personale;
- garantire la conservazione della documentazione;
- controllare che le violazioni dei dati personali siano documentate ed eventualmente notificate;
- controllare che si effettui la valutazione d'impatto preventiva;
- controllare che sia dato seguito alle richieste dell'autorità di controllo e fungere da punto di contatto con essa:
- Predisporre, gestire, controllare e manutenere il Sistema di Gestione Privacy Aziendale.

PRIVACY:
COME FARE A SCUOLA

REGISTRO ELETTRONICO E CODICE DELL'AMMINISTRAZIONE DIGITALE (CAD)

- Il piano "**e-Gov 2012**" ha definito una serie di **obiettivi per la cd. "digitalizzazione" della Pubblica Amministrazione** rispondenti alle necessità di semplificazione, riduzione delle spese e degli sprechi, migliore organizzazione delle risorse.
- Uno degli obiettivi da attuare riguarda proprio **l'informatizzazione di una serie di servizi di natura scolastica**: alcuni di essi - come il **registro** - già presenti nella versione tradizionale cartacea ed "aggiornati" alla tecnologia in uso, ed altri - come la prenotazione dei colloqui con i docenti - di nuova introduzione.

- Con tale intervento normativo, il legislatore ha di fatto attribuito **valore legale ai documenti che la Pubblica Amministrazione produce in formato digitale**.
- **Il documento informatico è sostanzialmente equiparato a quello cartaceo**, **purché sussistano certe condizioni di sicurezza**.
- Si prenda ad esempio la questione del **registro elettronico**. Indipendentemente dal *software* di gestione il registro elettronico **consiste nella trasposizione digitale del tradizionale registro cartaceo, cui aggiunge l'operatività in remoto o multi-accesso** (che consente ai docenti di operare da più postazioni a scuola o, al limite, anche da casa)
- I dati contenuti nel registro elettronico avranno pertanto il **medesimo valore legale delle annotazioni autografe iscritte sul tradizionale registro cartaceo**, a condizione che la "firma" del documento digitale sia, anch'essa, equiparata ad una firma apposta a mano.

Privacy-Trasparenza e Web

- Sono state aggiornate le linee guida del GdP relativamente alla privacy e alla trasparenza per le Pubbliche Amministrazioni.
- Tra le novità anche quella relativa all'indicizzazione nei motori di ricerca. Secondo quanto riportato nel nuovo documento, le PA dovranno adottare misure per **impedire l'indicizzazione dei dati sensibili** da parte dei motori di ricerca e il loro riutilizzo.
- Le Pa devono **pubblicare solo dati esatti, aggiornati e contestualizzati**, **e per un periodo di tempo congruo**.
- Prima di mettere on line sui propri siti informazioni, atti e documenti amministrativi contenenti dati personali, le amministrazioni **devono verificare che esista una norma di legge o di regolamento che ne preveda l'obbligo**.

PRIVACY:
MISURE FISICO-TECNICHE

- ~~Misure Minime~~, Idonee e Adeguate
- Sistemi Informativi orientati alla Sicurezza:
  - Password, Antivirus, Firewall, Backup (doppio, online e offline), Gestione file di LOG, Aggiornamento dei sistemi, Protezione fisica e logica della postazione, WiFi “sicuro”, etc.
- Misure Fisiche:
  - Portineria presidiata, registri d’accesso, badge, antifurto, armadi con chiave, vigilanza, etc.

Servizi Cloud

- I servizi Cloud tipo Onedrive o Google Drive facilitano considerevolmente la circolazione delle informazioni e dei sussidi didattici
- **Vanno usati con particolare attenzione**
- Sono GDPR compliance? Dove sono i dati? Chi vi accede? Cosa pubblico?
- Troppo facile l'accesso e troppo frequente il furto d'identità
- Attenzione: Cloud = Diffusione del dato = La responsabilità è di chi vi ha accesso e di chi pubblica e/o è tenuto alla sorveglianza

LA PRIVACY TRA I BANCHI DI SCUOLA

Le pubbliche amministrazioni, ed in particolar modo le scuole, sono fra i soggetti maggiormente coinvolti per una corretta implementazione di un adeguato sistema Privacy perché:

- **Trattano dati su larga scala;**
- **Trattano particolari categorie di dati personali;**
- **Trattano dati di minori**.

Nelle scuole, di ogni ordine e grado, vengono trattate quotidianamente numerose informazioni sugli studenti, sul personale e sulle loro rispettive famiglie, sui loro problemi sanitari o di disagio sociale, sulle abitudini alimentari.

A volte basta poco per violare, anche involontariamente, la riservatezza e/o la dignità di una persona: un PDP, un PEI, un verbale di classe (contenente riferimenti a particolari categorie di dati personali) lasciato su un computer privo delle adeguate misure di sicurezza, un tabellone scolastico con riferimenti indiretti sulle condizioni di salute degli studenti, la comunicazione di dati personali fra enti pubblici o soggetti privati privi di titolo.

VOTI ED ESAMI

Temi in Classe

- Non commette violazione della privacy l'insegnante che assegna ai propri alunni lo svolgimento di **temi in classe riguardanti il loro mondo personale o familiare**.
- Nel momento in cui gli elaborati vengono **letti in classe** – specialmente se sono presenti 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**.

VOTI SCOLASTICI, SCRUTINI, TABELLONI, ESAMI DI STATO

- **Non esiste alcun provvedimento del Garante che imponga di tenere segreti i voti** dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato, perché le informazioni sul rendimento scolastico sono soggette a un regime di trasparenza.
- Il regime attuale relativo alla conoscibilità dei risultati degli esami di maturità è stabilito dal Ministero dell'istruzione. Per il principio di trasparenza a garanzia di ciascuno, **i voti degli scrutini e degli esami devono essere pubblicati nell'albo degli istituti**.

- È necessario prestare attenzione, però, a **non fornire – anche indirettamente – informazioni sulle condizioni di salute degli studenti, o altri dati personali non pertinenti**. Ad esempio, il riferimento alle “prove differenziate” sostenute dagli studenti portatori di handicap non va inserito nei tabelloni affissi all’albo dell’istituto, ma deve essere indicato solamente nell’attestazione da rilasciare allo studente.

INFORMAZIONI SUGLI STUDENTI

CIRCOLARI E COMUNICAZIONI SCOLASTICHE

- Il **diritto/dovere di informare** le famiglie sull'attività e sugli avvenimenti della vita scolastica deve essere **sempre bilanciato con l'esigenza di tutelare** la personalità dei minori.
- È quindi necessario, ad esempio, **evitare di inserire nelle comunicazioni scolastiche elementi che consentano di risalire, anche indirettamente, all'identità di minori** coinvolti in vicende particolarmente delicate, **soprattutto nel momento in cui tali comunicazioni vengono gestite con mezzi non adeguati**.

ORIENTAMENTO, FORMAZIONE E INSERIMENTO PROFESSIONALE

- **Su richiesta delle famiglie o degli studenti maggiorenni** interessati, le scuole possono comunicare, anche a privati e per via telematica, **i dati relativi ai loro risultati scolastici per aiutarli nell'orientamento**, la formazione e l'inserimento professionale anche all'estero, purché la richiesta, da parte delle aziende, venga fatta con delle procedure adeguate stabilite dall'Istituto e non dall'azienda.

QUESTIONARI PER ATTIVITÀ DI RICERCA

Svolgere attività di ricerca con la raccolta di informazioni personali, spesso anche sensibili, tramite questionari da sottoporre agli alunni, **è consentito soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati** sulle **modalità di trattamento e conservazione dei dati raccolti e sulle misure di sicurezza adottate**. Gli intervistati, inoltre, devono sempre avere la facoltà di non aderire all'iniziativa.

FOTO
AUDIO
VIDEO

ATTIVITA' DIDATTICHE

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.

Va però prestata particolare attenzione all'utilizzo di immagini e video degli alunni da parte della scuola.

Il Garante della privacy sembra abbia chiarito, così come per qualsiasi altro fine istituzionale, che la scuola non deve chiedere il consenso per la pubblicazione sul sito internet dell'istituto di foto degli studenti, perché si suppone che lo faccia per fini istituzionali, partendo inoltre dal presupposto che quello che regola la pubblicazione delle foto da parte della scuola, nella sua qualità di Pubblica Amministrazione, deve essere il principio di "non eccedenza" (e ovviamente il buonsenso).

Oltre a ciò il Garante, per attribuire il carattere istituzionale alla pubblicazione delle fotografie nel sito web della scuola, ad esempio propone di usare il PTOF.

Ovviamente non è sufficiente riportare una annotazione generica nel PTOF per tutelare da Scuola. Sarà necessario quantomeno:

- **dimostrare che la pubblicazione delle fotografie o video è indispensabile per la valenza di uno o più progetti didattici. A tale scopo occorre descrivere nel PTOF, singolarmente per ogni progetto coinvolto, i motivi didattici che rendono necessaria la pubblicazione delle fotografie;**
- **approvare un regolamento che individui i contesti istituzionali in cui sia lecita la pubblicazione delle fotografie o video in cui sono riconoscibili gli studenti (il regolamento e la delibera di approvazione del Consiglio di Istituto dovranno, come d'uso, essere pubblicate all'albo della scuola);**
- **Limitando le foto sempre a gruppi di soggetti e non a singoli studenti;**
- **Limitando il contesto al solo sito istituzionale su pagine tassativamente non indicizzate dai motori di ricerca o meglio ancora all'interno di aree riservate;**
- **Valutando, sempre all'interno del regolamento, di non pubblicare comunque foto di soggetti particolarmente a rischio, se non previo esplicito consenso da parte di coloro i quali esercitano la responsabilità genitoriale;**
- **Limitando il numero delle foto al minimo, sempre corredate da un trafiletto che ne spieghi il relativo progetto didattico.**

REGISTRAZIONE DELLA LEZIONE

- **È possibile registrare la lezione esclusivamente per scopi personali**, ad esempio per motivi di studio individuale. **Per ogni altro utilizzo** o eventuale diffusione, anche su Internet, **è necessario prima informare adeguatamente le persone coinvolte** nella registrazione (professori, studenti…), e ottenere il loro esplicito consenso. Nell'ambito dell'autonomia scolastica, gli istituti possono decidere di regolamentare diversamente o anche di inibire gli apparecchi in grado di registrare prevedendone le eventuali eccezioni all'interno del regolamento d'Istituto.

SICUREZZA E CONTROLLO

Le graduatorie

- Il Garante è intervenuto più volte contro illeciti compiuti nella pubblicazione on line di graduatorie di vario tipo, le quali **spesso contengono dati personali non pertinenti o eccedenti** le finalità istituzionali perseguite.
- Alcuni Comuni, **ad esempio**, hanno **pubblicato on line le graduatorie di chi ha diritto ad usufruire del servizio di scuolabus** includendo tra le varie informazioni liberamente accessibili, non solo i dati identificativi dei bambini, **ma anche l'indirizzo di residenza e il luogo preciso dove lo scuolabus li avrebbe fatti salire e scendere**. La diffusione di questi dati, oltre a comportare una violazione della normativa, può rendere i minori facile preda di malintenzionati.

- Un altro caso frequente riguarda la **pubblicazione sui siti Internet degli istituti delle graduatorie di docenti e personale amministrativo** tecnico e ausiliario (ATA) per consentire a chi ambisce a incarichi e supplenze di conoscere la propria posizione e punteggio. Tali liste, giustamente accessibili a tutti, **non devono però contenere**, come in diversi casi segnalati al Garante, **i numeri di telefono e gli indirizzi privati dei candidati**. Questa illecita diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori a forme di stalking o a possibili furti di identità.

Le aree di rischio

Quali sono in una scuola le aree maggiormente soggette a rischio?

1. La documentazione utilizzata negli uffici per la gestione della didattica e del personale è spesso obsoleta o derivata dal 'copia ed incolla' da Internet. I pochi moduli ministeriali non sono assolutamente sufficienti a gestire le molteplici casistiche che vengono quotidianamente trattate in questi uffici. Una corretta ed uniforme gestione documentale può aiutare a prevenire i rischi e le sanzioni derivanti dall'errato utilizzo dei dati.
2. Sempre nei locali della segreteria e negli archivi storici è opportuno che gli arredi che contengono particolari categorie di dati personali siano debitamente chiudibili a chiave.
3. La sala insegnanti, l'aula di sostegno così come i computer nelle aule didattiche o nei laboratori informatici, spesso e volentieri, sono un vero e proprio ricettacolo di rischi, in quanto, se la scuola non dispone di un'adeguata infrastruttura informatica, vengono lasciati incustoditi dati nei computer utilizzati promiscuamente (quasi sempre collegati ad internet) da molteplici utenti, ma anche sui tavoli, ai quali dati possono accedere persone che non ne hanno titolo o peggio ancora gli studenti.
4. Il sito internet spesso viene sottovalutato e gestito in maniera non corretta, sia dal punto di vista privacy che per quanto riguarda la normativa sulla trasparenza. Il sito internet è la 'vetrina sul mondo'. Chi organizza una eventuale verifica ispettiva nei confronti di un ente o di un'azienda, per prima cosa analizza il sito; se questo non è a norma neanche l'organizzazione molto probabilmente non lo sarà.

Ministero
Istruzione
Università
Ricerca

GEMINI
STUDIO PRIVACY

GRAZIE

GEMINI CONSULT SRL
Sede legale: Via F.M. Preti 2/a - 31033 Castelfranco V.to TV
Sede operativa: via Europa 3 – 31052 Maserada sul Piave TV
Tel. 0422/877411 – mail: gemini@geminiconsult.it