La gestione della Privacy

Obblighi, responsabilità e sanzioni per le scuole

a cura del dott. GIAMBATTISTA ROSATO

Esperto giuridico ed informatico, formatore progetto "IoConto" MIUR, DPO, direttore amministrativo, già direttore nucleo Puglia INDIRE.

2025/2026

aggiornamento in-formativo

La formazione dei dipendenti sul GDPR: è obbligatoria?

La risposta è SI.

L'art. 29 del GDPR 679/2016, adottato dalla Commissione Europea per tutelare i dati personali dei cittadini, è molto chiaro:

"il responsabile del trattamento, o chiunque agisca sotto la sua autorità o sotto quella del titolare (responsabile del trattamento), che abbia accesso ai dati personali non può trattare tali dati ***se non è istruito in tal senso dal titolare"*****.**

La formazione dei dipendenti sul GDPR

Cosa significa:

Tutti coloro che nell'ambito dell'attività lavorativa entrano in contatto con «dati personali» devono ricevere una formazione specifica per conoscere – in linea generale -, quali sono gli adempimenti imposti dal GDPR e perché è importante eseguirli.

La formazione dei dipendenti sul GDPR

Cosa succede se non avviene la formazione del personale in materia di privacy?

Si è sanzionabile dal Garante per la privacy e le multe sono molto **«salate»**!!!

Non vanno sottovalutate le sanzioni correlate ad eventuale inadempienza.

Infatti, in caso di controlli che riscontrassero l'assenza di un adeguato piano formativo, ai sensi dell'art. 83 del GDPR può scattare la sanzione amministrativa pecuniaria fino a 10 milioni di euro o, per le imprese, fino al 2 % del fatturato mondiale annuo dell'anno precedente.

La formazione dei dipendenti sul GDPR

L'art 32 del GDPR ribadisce il concetto: chi non è adeguatamente formato non deve avere accesso a dati personali

Infatti, l'art.32 del GDPR rubricato come “Sicurezza del trattamento” è molto importante sul tema, sopratutto per la specifica del paragrafo 4 secondo cui: *“il titolare del trattamento ed il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri*”.

La formazione dei dipendenti sul GDPR

La formazione del personale sul GDPR è uno dei tasselli essenziali per la conformità al GDPR stesso.

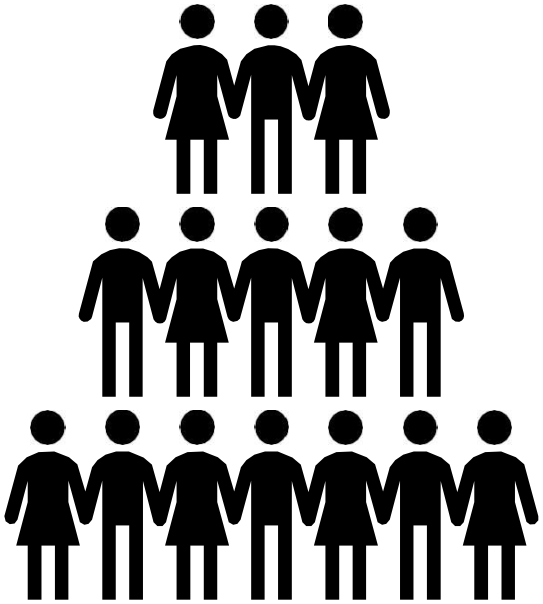
Il piano formativo costituisce, insieme ad altri elementi, uno dei tasselli fondamentali per la conformità al GDPR, secondo il **principio di accountability (o responsabilizzazione)** , inteso come la capacità del titolare di dimostrare di aver adottato tutte le misure adeguate per la protezione dei dati personali trattati oltre che tutti i sistemi organizzativi interni necessari, compresa la sensibilizzazione del personale.

La formazione non deve essere considerata come un adempimento burocratico ma va intesa alla stregua di un'opportunità per rendere consapevoli tutti gli operatori all'interno dell'organizzazione dei possibili rischi connessi al trattamento dei dati al fine di evitare anche i rischi di sanzioni amministrative.

La formazione dei dipendenti sul GDPR

La formazione costituisce, pertanto, una misura di sicurezza per le organizzazioni, un onere a carico del titolare, un diritto e dovere per i dipendenti e i collaboratori.

La Scuola a prova di privacy



La Scuola con l'innovazione tecnologica ha rivoluzionato i processi formativi – dall'uso del web ai tablet su cui consultare i libri, dai sistemi di messaggistica e i social media al registro elettronico – resta centrale la necessità di riaffermare quotidianamente, anche in ambito scolastico, quei principi di civiltà e rispetto, come la riservatezza e la dignità della persona, che devono sempre essere al centro della formazione di ogni cittadino di oggi e di domani.

Molte sono le novità introdotte dal GDPR, la cui analisi ci porta a chiarire dubbi o fraintendimenti legati al trattamento dei dati nelle Scuole – dall'attività didattica alla gestione dei rapporti di lavoro – oltre che a fornire alcune indicazioni e suggerimenti su come aiutare i più giovani a tutelarsi di fronte ai rischi connessi allo sviluppo del mondo digitale.

Il diritto alla riservatezza: la privacy

Il trattamento dei dati personali quale protezione delle persone fisiche è un diritto fondamentale ovvero il "*diritto di difendere la propria sfera privata*" in stretto collegamento con l'uso che gli altri fanno delle informazioni che riguardano il singolo individuo.

Il diritto della persona alla riservatezza, quale diritto fondamentale, va bilanciato con la finalità della trasparenza amministrativa operando non come prerogativa assoluta ma alla luce della funzione sociale contemperata con altri diritti fondamentali in ossequio al principio di proporzionalità.

Infatti, la trasparenza delle informazioni e degli atti della Pubblica Amministrazione coinvolgendo necessariamente anche singoli individui, deve controbilanciarsi necessariamente nell'alveo degli interessi legittimi contrapposti.

General data protection regulation (GDPR)

Il Regolamento (UE) 2016/6791 del Parlamento europeo e del Consiglio, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali (GDPR, o RGPD) è entrato in vigore il 27 aprile 2016 e diventato pienamente applicabile in tutti gli Stati membri dell'Unione Europea dal 25 maggio 2018.

Il Codice della Privacy di cui al d. lgs. 196/2003 e ss. mm. ii., per l'effetto della diretta applicazione del Regolamento UE 2016/679, ha perso la sua centralità come unica fonte normativa, pur rimanendo un testo di notevole importanza in materia.

General data protection regulation (GDPR)

Il GDPR si snoda in un percorso binario – tutela della privacy e protezione dei dati:

1. **tutela della privacy**: riservatezza nell'uso delle informazioni personali di terzi;
2. **protezione dei dati**: obblighi relativi alle misure di sicurezza nella gestione informatica dei dati.

Nel GDPR si individuano due principi cardine:

- ***accountability*** (cd. responsabilizzazione);
- **sicurezza dei dati personali** (adozione di adeguate misure tecniche e organizzative).

General data protection regulation (GDPR)

L'**accountability** – art. 5 comma 2 del GDPR e C 74 - prevede che il titolare del trattamento debba assicurare ed essere in grado di dimostrare di aver rispettato i principi applicabili al trattamento dei dati personali. Allo stesso modo, spetterà al titolare del trattamento dei dati personali valutare i rischi incombenti sui trattamenti e individuare le misure tecniche e organizzative adeguate al fine di escludere o, quantomeno, attenuare tali rischi.

L'**accountability** è uno dei pilastri fondamentali del GDPR, esso infatti cambia il precedente sistema formalistico introducendo la responsabilizzazione (*accountability*) del Titolare dei dati.

General data protection regulation (GDPR)

Il Titolare dei dati è infatti colui che ha la responsabilità di decidere le modalità con cui uniformarsi al GDPR.

Egli deve essere in grado di dimostrare, attraverso un idoneo sistema documentale di gestione della privacy, la conformità al GDPR e le motivazioni delle scelte effettuate.

Deve quindi tenere conto della natura, dell'ambito, del contesto delle finalità e dei rischi dei trattamenti pianificati.

Il GDPR, nella parte in cui si occupa del tema della sicurezza del trattamento, prevede che il titolare e il responsabile del trattamento debbano adottare "*misure tecniche e organizzative*".

General data protection regulation (GDPR)

Nel GDPR non è più prevista un'elencazione puntuale delle misure di sicurezza (come accadeva con le misure minime di sicurezza previste dall'All. B del Codice della Privacy italiano), ma ci si "limita" a offrire un criterio per l'individuazione delle specifiche misure tecniche e organizzative da approntare, volta per volta, al trattamento.

Il GDPR, infatti, prescrive l'adozione di misure di sicurezza, tecniche e organizzative, che siano adeguate a fronteggiare escludendolo o limitandolo al massimo il rischio incombente sui dati personali oggetto di ogni singolo trattamento posto in essere.

Lo scopo sotteso è la tutela dei diritti e le libertà delle persone fisiche contro i rischi che possano derivare da un trattamento non corretto dei dati personali.

General data protection regulation (GDPR)

Pertanto, è necessario mettere in atto, sulla base di quanto previsto dall'art. 25, par. 1 del Regolamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento, misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie previste dal Regolamento, nonché a tutelare i diritti degli interessati. Inoltre, si devono porre in essere, sulla base di quanto previsto dall'art. 25, par. 2 del Regolamento, misure tecniche e organizzative adeguate per garantire che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari per ogni specifica finalità del trattamento nel rispetto del principio della *minimizzazione del dato*, assicurando la *liceità del trattamento*.

General data protection regulation (GDPR)

La privacy come elemento di progettazione delle misure tecniche ed organizzative (**privacy by design**), anche prima che il trattamento inizi in funzione del tipo di dati trattati ovvero un approccio secondo cui si devono predisporre i necessari strumenti di tutela (ad es. pseudonomizzazione) e protezione dei dati personali prima di iniziare il trattamento, con il fine di prevenire, più che correggere in un momento successivo, una possibile violazione.

E' necessaria una valutazione del rischio (*risk based approach*) prima di iniziare il trattamento.

Per impostazione predefinita i "titolari del trattamento" dovrebbero trattare solo i dati personali nella misura necessaria e sufficiente per le finalità previste e per il periodo strettamente necessario a tali fini (**privacy by default**). 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 ovvero si dovrebbero trattare i dati personali nella misura necessaria e sufficiente per le finalità previste del trattamento e per il periodo strettamente necessario a tale scopo.

Occorre, quindi, progettare il sistema di trattamento di dati garantendo la non eccessività dei dati raccolti.

General data protection regulation (GDPR)

La **gestione dei dati personali** non è più solo un adempimento ma **diventa un processo** che deve essere gestito modificando l'organizzazione.

Si va verso la predisposizione di un **modello organizzativo** nella gestione dei dati personali finalizzato a prevenire i rischi di utilizzo illecito dei dati.

La disciplina si applica ai trattamenti di dati delle persone fisiche, non essendo "dati personali" quelli delle persone giuridiche. L'art. 2, infatti, precisa che il Regolamento si applica anche ai trattamenti non automatizzati di dati personali, purché siano "*contenuti in un archivio o destinati a figurarvi*".

Ne consegue che tutti i trattamenti di dati personali, anche quelli meramente cartacei sono soggetti all'applicazione del Regolamento, infatti l'eventuale smarrimento o la sottrazione di un fascicolo cartaceo contenente dati personali, rappresenterà, pertanto, una violazione di dati personali, tanto quanto la sottrazione dei medesimi dati contenuti in un archivio informatico.

Il GDPR definisce dato personale qualsiasi informazione riguardante una persona fisica identificata o identificabile: cd. "interessato".

General data protection regulation (GDPR)

La persona fisica si considera identificabile quando possa essere individuata, direttamente o indirettamente, con riferimento a dati identificativi, quali il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo on line o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Il GDPR distingue in particolare tre categorie di dati personali:

- **dati comuni**: sono individuati in negativo, in quanto sono tutti quei dati personali che non rientrano nelle categorie particolari, o che non siano dati inerenti a condanne penali e reati;

- **categorie particolari di dati**: coincidono, seppur parzialmente, con i "vecchi" dati sensibili sono rappresentate da tutti quei dati che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche o l'appartenenza sindacale, dati genetici, dati biometrici, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona. L'art. 9 del GDPR stabilisce un generale divieto di trattamento, temperato da alcune eccezioni (vds in seguito base legale del trattamento dei dati;

- **dati relativi a condanne penali e reati**: i dati giudiziari - art. 10 del GDPR e art. 2-*octies* del Codice Privacy, sebbene non rientrino tra le particolari categorie di dati, meritano particolare attenzione; concernono i dati relativi alle condanne penali e ai reati o connesse a misure di sicurezza ed il loro regime è caratterizzato da importanti restrizioni, previste sia dal GDPR che dalla normativa nazionale.

General data protection regulation (GDPR)

Il Regolamento, inoltre, da questa categorizzazione, definisce quattro diverse fattispecie in base alla modalità di rilevazione.

I dati possono essere:

- 1. ***Provided***, cioè forniti consapevolmente dall'utente (es. registrazione)
- 2. ***Observed***, cioè desumibili dalla navigazione dell'utente, ovvero informazioni che non sono raccolte per essere associate a interessati identificati, ma che per loro stessa natura potrebbero, attraverso elaborazioni ed associazioni con dati detenuti da terzi, permettere di identificare gli utenti.
- 3. ***Derived***, cioè derivati da una precedente raccolta (es. profilazione)
- 4. I***nferred***, cioè aggregati su cui vengono fatte previsioni statistiche.

È fondamentale, difendere questi dati da un possibile accesso illecito, così come è estremamente rilevante che il processo di acquisizione sia il più sicuro possibile e che gli errori vengano limitati.

General data protection regulation (GDPR)

I sei principi fondamentali ai quali il GDPR prevede che si debba ottemperare per proteggere i dati:

1. Liceità, correttezza e trasparenza nei confronti dell'Interessato.

2. Limitazione delle finalità, ovvero i dati devono essere raccolti per finalità determinate, esplicite, legittime e trattati in base ad esse.

3. Minimizzazione dei dati, che devono essere adeguati, pertinenti e limitati a quanto necessario per le finalità dichiarate.

4. Esattezza, ciò implica che i dati siano precisi ed aggiornati oppure tempestivamente rettificati o eliminati.

5. Limitazione della conservazione, che permette di conservare i dati solo per il tempo necessario alla finalità del trattamento.

6. Integrità e riservatezza, che devono tutelare i dati dalla diffusione, dalla perdita e dalla distruzione.

Privacy e fondamento Costituzionale

Pur non essendo espressamente menzionato nella Costituzione italiana, il diritto alla privacy è ricavabile da diversi principi costituzionali:

- **Art. 2 Cost.** – tutela dei diritti inviolabili dell'uomo;
- **Art. 13 Cost.** – libertà personale;
- **Art. 14 Cost.** – inviolabilità del domicilio;
- **Art. 15 Cost.** – segretezza della corrispondenza e delle comunicazioni;
- **Art. 21 Cost.** – libertà di manifestazione del pensiero, bilanciata con la tutela dell'onore e della reputazione.

A partire da tali valori, la giurisprudenza ha riconosciuto la riservatezza come diritto fondamentale, poi disciplinato organicamente dal legislatore.

Regole Generali

Prima di tutto … Trasparenza!

Tutte le scuole hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, docenti e altro personale) come vengono trattati i loro dati personali.

Il linguaggio dell'informativa deve essere facilmente comprensibile anche dai minori e deve contenere, in particolare, gli elementi essenziali del trattamento, specificando che le finalità perseguite sono limitate esclusivamente al perseguimento delle funzioni istituzionali necessarie per assicurare il diritto all'istruzione e alla formazione attraverso l'erogazione dell'attività didattica.

TRATTAMENTO DEI DATI

Tutte le scuole possono trattare i dati personali degli studenti, anche relativi a categorie particolari, funzionali all'attività didattica e formativa, per il perseguimento di specifiche finalità istituzionali quando espressamente previsto dalla normativa di settore.

Privacy e Pubblica Amministrazione

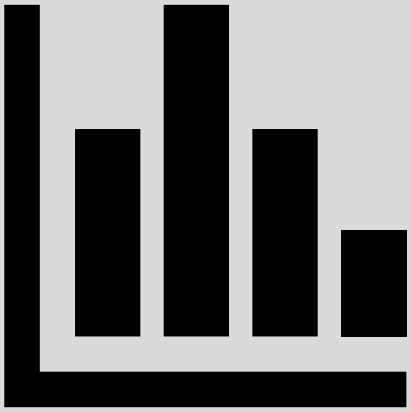
Le pubbliche amministrazioni e quindi le Scuole sono vincolate a un equilibrio delicato tra **trasparenza** e **riservatezza**.

La trasparenza amministrativa non può mai tradursi in una diffusione indebita di dati personali non pertinenti o eccedenti rispetto alle finalità di legge.

Nel contesto scolastico, ad esempio, il trattamento dei dati deve tener conto:

- della particolare protezione dei **minori**;
- della necessità di ridurre al minimo la diffusione di dati particolari (sensibili) su studenti, famiglie e personale scolastico;
- della pubblicazione selettiva e proporzionata degli atti amministrativi.

CATEGORIE PARTICOLARI DI DATI RELATIVI AD ALUNNI



- ***Origini razziali ed etniche***
- ***Convinzioni religiose***
- ***Stato di salute***
- ***Opinioni politiche***
- ***Dati personali relativi a condanne penali e reati***

La base giuridica del trattamento

È costituita, ai sensi dell'art. 6, lett. e), del Regolamento UE n. 679/2016 dall'esecuzione di **un compito di interesse pubblico e dall'esercizio dei pubblici poteri**.

Le Istituzioni Scolastiche, durante lo svolgimento dei loro compiti, hanno il dovere di **rispettare** la privacy e **tutelare e proteggere** i dati personali che trattano, in particolare perché i dati afferiscono a soggetti generalmente minorenni.

Il trattamento dei dati, anche a protezione speciale, è giustificato per **motivi di interesse pubblico rilevante**.

La base giuridica del trattamento

L'art. 2 sexies del Codice Privacy aggiornato precisa che: "*I trattamenti delle categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, del Regolamento, necessari per motivi di interesse pubblico rilevante ai sensi del paragrafo 2, lettera g), del medesimo articolo, sono ammessi qualora siano* ***previsti dal diritto dell'Unione europea ovvero, nell'ordinamento interno, da disposizioni di legge o, nei casi previsti dalla legge, di regolamento*** *che specifichino i tipi di dati che possono essere trattati, le operazioni eseguibili e il motivo di interesse pubblico rilevante, nonché le misure appropriate e specifiche per tutelare i diritti fondamentali e gli interessi dell'interessato.*

2. Fermo quanto previsto dal comma 1, si considera rilevante l'interesse pubblico relativo a trattamenti effettuati da soggetti che svolgono compiti di interesse pubblico o connessi all'esercizio di pubblici poteri nelle seguenti materie: bb) ***istruzione e formazione in ambito scolastico, professionale, superiore o universitario***".

La base giuridica del trattamento

Art. 5 – Base giuridica (principio di leicità) - il trattamento è lecito solo se 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 e 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 e 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) - lettera f non per autorità pubbliche nell’esercizio delle loro funzioni.

La base giuridica del trattamento

Base giuridica – in sintesi a scuola consenso o no?

Il Dirigente (titolare del trattamento) può trattare i dati **senza consenso**:

• quando il trattamento interessa l'esecuzione di un contratto di cui l'interessato è parte (fornitori, esperti esterni, eccetera);

• per tutte le attività che è obbligato per legge ad effettuare;

• quando il trattamento è necessario alle finalità istituzionali (es. attività entro PTOF).

Per il tutti gli altri trattamenti: **necessario consenso**

Esempio:

- Trattamento foto / video

- Trasmissione dati per scopo di inserimento in scuole di ordine superiore

- Attività di allocazione post-diploma

- Attività progettuali non riportate nel PTOF

Oggetto del trattamento

Sono, ai sensi dell'art. 4, n. 1 del Regolamento UE n. 679/2016, i dati individuati nell'allegato al D.M. n. 108/2020, ovvero:

– dati anagrafici (quali codice fiscale, nome, cognome, data di nascita, comune di nascita, sesso);

– dati inerenti alla professionalità del docente (quali nome del titolo di studio, localizzazione del conseguimento del titolo di studio, riconoscimento del titolo estero, anno di conseguimento del titolo di studio, classe di concorso di abilitazione, livello scolastico scuola di sostegno);

– dati inerenti all'inquadramento contrattuale del docente (quali tipologia di contratto/prestazione, tempo determinato/indeterminato, CCNL di riferimento, data inizio e fine contratto/prestazione);

– dati relativi al servizio prestato dal docente (quali tipologia di insegnamento, classe di concorso, materie di insegnamento, ore settimanali, eventuali note);

– dati relativi alla scuola di riferimento (quali codice, denominazione, livello).

Non sono trattati dati ulteriori rispetto a quelli puntualmente individuati.

Oggetto del trattamento

Il trattamento viene effettuato attraverso strumenti automatizzati (ad es. utilizzando procedure e supporti elettronici) e/o manualmente (ad es. su supporto cartaceo) per il tempo strettamente necessario a conseguire gli scopi per i quali i dati sono stati raccolti e, comunque, con l'adozione di specifiche misure di sicurezza idonee ad evitare qualsiasi violazione dei dati personali, quali la perdita dei dati, usi illeciti o non corretti ed accessi non autorizzati.

Tuttavia, tali misure, per la natura del mezzo di trasmissione online, non possono limitare o escludere in assoluto qualsiasi rischio di accesso non consentito o di dispersione dei dati.

Soggetti autorizzati dell'Amministrazione centrale e/o periferica sono i dipendenti e collaboratori autorizzati del Responsabile del trattamento.

Non sono previsti trasferimenti di dati personali verso paesi terzi o organizzazioni internazionali.

Figure previste dal Regolamento

Titolare del Trattamento è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art. 4. par. 1, n. 7 del Regolamento). Nell'ambito dell'istituzione scolastica questa figura è identificata nella persona del Dirigente scolastico.

Responsabile del trattamento è la persona fisica, giuridica, pubblica amministrazione o ente che tratta i dati personali per conto del titolare del trattamento (art. 4, par. 1, n. 8 del Regolamento). Pertanto, il responsabile del trattamento è un soggetto terzo che tratta dati personali per conto del titolare, mettendo in atto misure di sicurezza adeguate di tipo tecnico ed organizzativo. Nell'ambito dell'istituzione scolastica questa figura è identificata nei fornitori delle piattaforme o dei servizi per la Didattica Digitale Integrata e Interattiva (DDII).

Responsabile della Protezione dei Dati personali (RPD), è la figura prevista dall'art. 37 del Regolamento, assicura l'applicazione della normativa in materia di protezione dei dati personali in relazione ai trattamenti svolti dal titolare del trattamento. La nomina è obbligatoria per le pubbliche amministrazioni; può essere una figura sia interna che esterna (con apposito contratto di servizi) - è designato, secondo quanto prevede l'art. 37, in funzione delle qualità professionali e, in particolare, della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti che gli sono assegnati sulla base del GDPR.

Figure previste dal Regolamento

I compiti sono elencati all'art. 39 del GDPR, e, precisamente: offre consulenza a titolare, responsabile e dipendenti; fornisce il parere (se richiesto) sulla valutazione d'impatto ex art. 35 del GDPR; sorveglia sul rispetto della disciplina sulla protezione dati e sulle politiche del titolare in materia di protezione dei dati personali, compresa la sensibilizzazione e la formazione; coopera con l'Autorità Garante, e funge da punto di contatto. Il Responsabile della Protezione dei Dati deve essere tempestivamente coinvolto in tutte le questioni riguardanti il trattamento di dati personali.

Una sua funzione importante è quella legata al contatto con gli interessati, i quali possono interpellarlo per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti. La figura è circondata da specifiche cautele: egli, infatti, non deve svolgere altri compiti e funzioni che ingenerino conflitto d'interessi, è autonomo, non può ricevere direttive o istruzioni, non può essere rimosso per l'adempimento dei propri compiti, e riferisce direttamente al vertice gerarchico.

I designati e gli autorizzati

Il D.lgs. 101/2018, introducendo nel Codice Privacy l'art. 2-*quaterdecies*, ha provveduto a individuare in dettaglio le attribuzioni di funzioni e compiti in materia di trattamento di dati personali.

I designati - I "soggetti designati" previsti dal primo comma dell'art. 2-*quaterdecies*, sono le persone fisiche a cui il titolare o il responsabile attribuiscono specifici compiti e funzioni connessi al trattamento. Questi compiti e funzioni, nel rispetto del principio di responsabilizzazione, devono essere esplicitamente indicati, delimitando in tal modo l'ambito del trattamento.

Gli autorizzati - Il secondo comma dell'art. 2-*quaterdecies*, ricollegandosi agli artt. 29 e 32 del GDPR, prevede che il titolare o il responsabile) del trattamento debbano individuare le modalità più opportune per autorizzare al trattamento dei dati personali le persone che operano sotto la loro autorità diretta e riceva specifiche istruzioni, accompagnate da idonea formazione.

I designati e gli autorizzati

Nell'ambito delle organizzazioni complesse, pertanto, occorre individuare i soggetti designati, a cui attribuire specifici compiti e funzioni, e provvedere a fornire idonee e dettagliate istruzioni a tutti coloro che trattano i dati sotto l'autorità del titolare stesso. Il singolo Istituto Scolastico nell'ambito della sua autonomia organizzativa può individuare – ai sensi dell'art. 2-*quaterdecies* del D.lgs. 196/2003 così come modificato dal D.lgs. 101/2018 – la soluzione più idonea a gestire, dal punto di vista organizzativo interno, la tutela dei dati personali di cui l'Istituto stesso sia titolare. In questa sua qualità, l'Istituto Scolastico, a mezzo del Dirigente Scolastico, adotta gli opportuni provvedimenti relativi all'ambito tecnico e organizzativo. Il Dirigente Scolastico potrà decidere di individuare uno o più designati al trattamento dei dati personali, oltre a dover individuare specificamente i soggetti autorizzati al trattamento dei dati personali di cui l'Istituto Scolastico sia titolare, fornendo a questi ultimi idonee e specifiche istruzioni sul trattamento dei dati personali.

Chiunque abbia accesso ai dati personali, sotto l'autorità del titolare o del responsabile, deve essere preliminarmente autorizzato e debitamente istruito: l'autorizzazione e le istruzioni, per ciascun soggetto o tipologia di soggetti, siano essi designati al trattamento o autorizzati al trattamento sono, in genere, contemplate nello stesso atto.

Per quanto riguarda gli autorizzati, le Linee Guida del MIUR di aprile 2019 prevedono che essi siano tenuti a conformare i trattamenti a loro assegnati alla normativa in materia di protezione dei dati personali e alle istruzioni ricevute, e che, in linea generale, siano tenuti a: trattare solo i dati personali necessari per ogni specifica finalità del trattamento; verificare la legittimità e correttezza dei trattamenti, valutando, in particolare, i rischi che gli stessi presentano e la natura dei dati personali da proteggere.

L’informativa

Il regolamento europeo prevede che, in base alla finalità del trattamento, il titolare debba fornire agli interessati, prima del trattamento, le informazioni richieste dalle norme (art. 12). Ciò avviene tramite l'informativa.

L'informativa è una comunicazione rivolta all'interessato che ha lo scopo di informare il cittadino, anche prima che diventi interessato, sulle finalità e le modalità dei trattamenti operati dal titolare del trattamento, essa è condizione, non tanto del rispetto del diritto individuale ad essere informato, quanto del dovere del titolare del trattamento di assicurare la trasparenza e correttezza dei trattamenti fin dalla fase di progettazione dei trattamenti stessi, e di essere in grado di comprovarlo in qualunque momento (**principio di accountability**).

L'informativa ha anche lo scopo di permettere che l'interessato possa rendere un valido consenso, se richiesto come base giuridica del trattamento. In questo caso l'informativa non è solo dovuta in base al principio di trasparenza e correttezza, ma è anche una condizione di legittimità del consenso.

L'informativa è dovuta ogni qual volta vi sia un trattamento di dati. L'obbligo di informare gli interessati va adempiuto prima o al massimo al momento di dare avvio alla raccolta dei dati. Non sussiste obbligo di fornire l'informativa se il trattamento riguarda dati anonimi (es. aggregati) o dati di enti o persone giuridiche (i cui dati non sono soggetti alla tutela prevista dal regolamento europeo).

La persona fisica che effettua il trattamento dei dati per attività a carattere esclusivamente personale e domestico, non è tenuta a fornire l'informativa.

L’informativa

Nel caso in cui i dati non siano raccolti direttamente presso l'interessato (art. 14 del Regolamento), l'informativa deve essere fornita entro un termine ragionevole, e comunque non oltre un mese dalla raccolta dei dati. Oppure va fatta al momento della comunicazione dei dati a terzi.

L'informativa deve avere il seguente contenuto minimo (articoli 13 e 14 del Regolamento europeo):

- categorie di dati trattati e finalità del trattamento (non le modalità del trattamento, ma quali dati vengono trattati divisi per categorie, a quale fine, per quanto tempo sono trattati, se i dati verranno trasferiti all'estero e, in questo caso, attraverso quali strumenti);

- la base giuridica del trattamento, quindi se si tratta di trattamento basato su consenso o giustificato da leggi, legittimi interessi (in questo caso specificando quale è il legittimo interesse), ecc. ..;

- natura obbligatoria o facoltativa del conferimento dei dati e le conseguenze di tale rifiuto (specificando che è possibile rifiutare il consenso a singoli trattamenti quali quelli a fini di marketing diretto);

- se il titolare ha intenzione di utilizzare i dati per una finalità diversa da quella per la quale sono stati raccolti;

- soggetti destinatari (anche per categorie) ai quali i dati possono essere comunicati e l’ambito di diffusione dei dati medesimi (l'indicazione di soggetti terzi non può essere generica);

- se il titolare ha intenzione di trasferire i dati in paesi extra UE, nel qual caso se esiste o meno una decisione di adeguatezza della Commissione UE (ovvero se la Commissione ha deciso che il paese terzo, un territorio o uno o più settori specifici all'interno del paese terzo, o l'organizzazione internazionale in questione garantiscono un livello di protezione adeguato, per cui il trasferimento non necessita di autorizzazioni specifiche);

- il periodo di conservazione dei dati oppure l'indicazione dei criteri per determinarlo;

- i diritti dell’interessato (diritto di accesso ai dati personali, di ottenere la rettifica o la cancellazione degli stessi o la limitazione del trattamento che lo riguardano, di opporsi al trattamento, di revocare il consenso, diritto di presentare reclamo all'autorità di controllo, eventuale diritto alla portabilità);

- dati identificativi (nome, denominazione o ragione sociale, domicilio o sede) del titolare del trattamento e, se designato, del responsabile per la protezione dei dati (DPO), quindi un recapito al quale gli interessati potranno rivolgersi per esercitare i propri diritti;

- se il trattamento comporta processi decisionali automatizzati (come la profilazione) deve essere specificato indicando anche la logica di tali processi decisionali e le conseguenze previste per l'interessato.

L’informativa

All'interno dell'informativa privacy devono essere indicati anche i riferimenti circostanziati inerenti i cookie che veicolano il sito, le modalità di disabilitazione dei cookie (es. tramite opzioni del browser), e nel caso di cookie di terze parti, il link alle pagine delle privacy policy dei servizi delle terze parti.

L'informativa cookie è una sezione dell'informativa privacy, non un documento separato.

L'informativa deve avere forma coincisa, deve essere chiara, facilmente accessibile ed intellegibile per l'interessato, eventualmente anche utilizzando immagini o icone. L'informativa deve essere resa per iscritto o con altri mezzi (anche elettronici, come per es., la posta elettronica).

Stralcio esemplificativo del Report dei trattamenti, relativo agli operatori socio sanitari presenti nella scuola

FINALITÀ, TIPOLOGIE E BASI GIURIDICHE	**Finalità**	L'operatore socio sanitario affianca e assiste l'alunno nello svolgimento delle regolari attività svolte in classe in ragione della particolare condizione in cui lo stesso si trova. L'attività di collaborazione ha durata dalla data di stipula del contratto per ogni singolo operatore socio sanitario. Durate tale periodo l'operatore parteciperà alle attività didattiche qualora ne venga richiesta la sua presenza. (Ai sensi dell'art.5 GDPR, i dati sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali - Da specificare)
	Tipologie	Dati relativi agli alunni

Il consenso dell'interessato

Una volta ricevuta l'informativa, nei casi previsti, l'Interessato può manifestare la sua volontà prestando il suo consenso al trattamento dei dati.

Per evitare confusione il GDPR sancisce al suo interno alcune caratteristiche imprescindibili alla base del consenso.

Il consenso, infatti, deve essere sempre:

- Libero, dunque privo di condizionamento
- Informato, ovvero preceduto da un'informativa
- Inequivocabile, ovvero deve esserci certezza che sia stato prestato
- Specifico per ciascuna finalità

Infine, bisogna sottolineare che il consenso non è obbligatorio e può essere revocato in ogni momento.

Il regolamento impone al Titolare del trattamento di dimostrare i consensi acquisiti.

Periodo di conservazione dei dati personali

Ai sensi dell'art. 5, par. 1, lett. e) del Regolamento UE n. 679/2016, al fine di garantire un trattamento corretto e trasparente, i dati sono conservati per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati e, comunque, per un periodo di tempo non superiore all'anno scolastico di riferimento.

I sistemi informatici e le procedure software preposte al funzionamento del sito acquisiscono, nel corso del loro normale esercizio, dati di navigazione la cui trasmissione è implicita nell'uso dei protocolli di comunicazione di internet.

L'uso di c.d. cookie di sessione è strettamente limitato alla trasmissione di identificativi di sessione necessari a consentire l'esplorazione sicura ed efficiente del portale e dei suoi servizi. I cookie di sessione utilizzati nel sito evitano il ricorso ad altre tecniche informatiche potenzialmente pregiudizievoli per la riservatezza della navigazione degli utenti e non consentono l'acquisizione di dati personali identificativi dell'utente.

Diritti degli interessati

Il Regolamento UE n. 679/2016 attribuisce ai soggetti interessati diversi diritti.

- il **diritto ad essere informati.** La persona a cui i dati si riferiscono ha cioè il diritto di sapere in modo chiaro e trasparente chi e come tratta i suoi dati personali;
- il **diritto di accedere ai propri dati personali.** L'Interessato può quindi riconoscere in ogni momento quali sono i dati personali trattati dal Titolare, per quali finalità e altre informazioni relative;
- il **diritto alla rettifica,** ovvero l'Interessato può chiedere modifiche ai propri dati personali qualora ritenga che non siano accurati o aggiornati;
- il **diritto di revoca, i**n qualsiasi momento il consenso precedentemente concesso;
- il **diritto di opporsi al trattamento**, totalmente o parzialmente (per alcuni specifici tipi o finalità di trattamento);
- il **diritto alla cancellazione**;
- il **diritto all'oblio.** Il diritto di cancellare informazioni rese pubbliche in passato ma per le quali è venuto meno l'interesse iniziale alla diffusione;
- il **diritto alla portabilità dei dati**, che conferisce all'Interessato la possibilità di ricevere i propri dati personali o chiederne il trasferimento tra un Titolare e l'altro.

Diritti degli interessati

Ogni persona, in relazione al trattamento dei dati che la riguardano, potrà rivolgersi al Titolare del trattamento per esercitare i suoi diritti.

Nel caso in cui ritenga che il trattamento dei dati personali sia compiuto in violazione di quanto previsto dal Regolamento UE n. 679/2016, vige il diritto di proporre *reclamo* al Garante, come previsto dall'art. 77 del Regolamento UE n. 679/2016 stesso, o di adire le opportune sedi giudiziarie ai sensi dell'art. 79 del Regolamento UE n. 679/2016.

GDPR

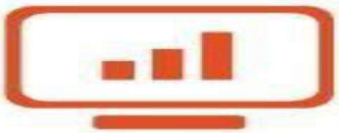
Ciclo del dato personale

Tipo dati raccolti

Raccogli troppi dati personali per raggiungere gli scopi prefissi?
Puoi ridurre il numero di dati raccolti ottenendo gli stessi risultati?

Finalità della raccolta

Quale è lo scopo della raccolta dei dati?
Lo hai specificato nell'informativa? Lo hai comunicato agli interessati?
Gli interessati sono a conoscenza di cosa accade ai loro dati quando te li conferiscono?

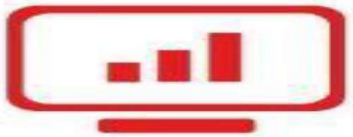


Aggiornamento dei dati

Hai una procedura per la verifica dell'esattezza dei dati e il loro eventuale aggiornamento?

Conservazione dei dati

Hai adottato misure per la sicurezza dei dati?
Ai dati possono accedere solo le persone autorizzate?
Hai adottato misure di backup dei dati?
Se il backup è nel Cloud, il fornitore del servizio è in regola con le norme?



Tempo di conservazione dei dati

Per quanto tempo i dati vengono conservati?
Hai procedure per la verifica che i dati siano conservati solo per il periodo necessario a raggiungere gli scopi prefissati?

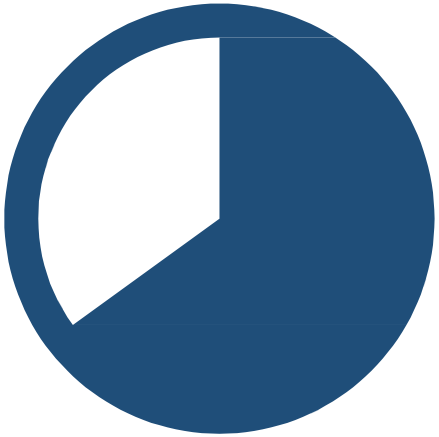
Diritti dell'interessato

Garantisci i diritti all'interessato (diritto di accesso, cancellazione e portabilità)?
Rispondi alle richieste dell'interessato nei tempi previsti dalle norme?

Regole Generali

Chi tratta i dati a Scuola?

All'interno della scuola, titolare del trattamento, il dirigente scolastico, in quanto legale rappresentante, prende decisioni sulle attività di trattamento da intraprendere e sulle modalità attraverso cui queste verranno svolte mediante il personale amministrativo e/o docente. Tale personale è quindi autorizzato a trattare i dati nell'ambito delle attività didattiche o amministrative.



… ogni attore del complesso mondo scuola, in ragione della funzione giuridica esercita, è autorizzato a trattare i dati a seguito di specifica autorizzazione al trattamento.

Il data breach

La violazione dei dati personali è definita dall'art. 4 comma 12 del GDPR come "*la violazione di sicurezza 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*". Si tratta, per l'appunto, di una violazione di sicurezza.

L'art. 29 WP – Working Group - (Gruppo dell'articolo 29 per la tutela dei dati), nelle proprie linee guida sulle violazioni di dati personali, distingue tre categorie, basandosi sui principi di sicurezza delle informazioni:

- – *violazioni della confidenzialità*: si verifica ad esempio quando un errore del sistema consente anche a terzi non autorizzati di accedere ai dati personali;

- – *violazioni dell'integrità*: consiste in una accidentale o non autorizzata alterazione dei dati;

- – *violazione della disponibilità*: si riscontra ad esempio quando l'azione di un ransomware (software malevolo che opera cifrando i dati dei sistemi, per richiedere poi un riscatto) provochi la perdita dell'accesso o la distruzione dei dati personali.

Sempre nell'ottica del rispetto del principio di responsabilizzazione, è indispensabile dotarsi di procedure specifiche per la gestione delle violazioni di dati personali, che individuino i soggetti coinvolti, e gli snodi principali, fino ad arrivare all'eventuale notificazione al Garante, o alla comunicazione agli interessati. In questo contesto è fondamentale la istituzione di un Registro delle violazioni; il GDPR all'art. 33, comma V, impone di documentare qualsiasi violazione con l'indicazione delle circostanze, delle conseguenze e dei successivi provvedimenti adottati.

Registro del trattamento

Il registro dei trattamenti – art 30 e C82 - è uno strumento indispensabile per ogni valutazione e analisi del rischio (principio di accountability).

L'onere della tenuta del registro è a carico del titolare e dei responsabili del trattamento.

Il registro deve essere tenuto in forma scritta, anche in formato elettronico e deve essere esibito su richiesta al Garante.

Nel registro devono essere indicati una lista di contenuti obbligatori elencati in art.30:

- il nome e i dati di contatto del titolare del trattamento e, ove applicabile, del contitolare del trattamento, del rappresentante del titolare del trattamento e del responsabile della protezione dei dati;
- le finalità del trattamento;
- una descrizione delle categorie di interessati e delle categorie di dati personali;
- le categorie di destinatari a cui i dati personali sono stati o saranno comunicati, compresi i destinatari di paesi terzi od organizzazioni internazionali;
- Gli eventuali trasferimenti di dati personali verso un paese terzo o un'organizzazione internazionale;
- I termini ultimi previsti per la cancellazione delle diverse categorie di dati;
- Una descrizione generale delle misure di sicurezza tecniche e organizzative.

Registro del trattamento

Il paragrafo 2 dell'articolo 30 del GDPR prevede che anche i responsabili del trattamento debbano tenere un registro simile in relazione alle attività svolte per conto del titolare.

Ci sono cause di esenzione ma numerosi pareri indicano l'opportunità di mantenere il registro in OGNI CASO per dimostrare la propria "accountability".

La tenuta del registro dei trattamenti, obbligatorio, in ambito scolastico ma **parte integrante di un sistema di corretta gestione dei dati personali**.

Il Miur, con nota n. 877 del 03/08/2018, ha trasmesso alle scuole uno schema di Registro delle attività di trattamento per le Scuole, fornendo anche una Guida operativa e una nota metodologica che illustra la metodologia specifica da applicare per la compilazione del registro.

Le attività di trattamento (es. gestione iscrizioni, gestione carriera scolastica alunni, gestione personale docente ...) svolte normalmente dalle istituzioni scolastiche sono dettagliatamente descritte nella Guida.

L’indirizzo di posta elettronica è dato personale, diffonderlo a scuola senza consenso è violazione della privacy. Scuola condannata

Una scuola aveva affisso all´albo e alle bacheche esterne della scuola il testo di una comunicazione elettronica contenente l´indirizzo privato di posta elettronica della sig.ra XY.

Nella sua ricostruzione in fatto rilevava l’Autorità procedente che l´istituto non ha ritenuto necessario eliminare l´indirizzo e-mail dalla lettera come pubblicata perché in quel contesto secondo la scuola il dato non poteva considerarsi riservato, ma parte integrante della comunicazione. La scuola sosteneva altresì che “la mail personale è sempre stata ampiamente utilizzata e quindi diffusa dall´interessata stessa, per tutte le comunicazioni inerenti il suo compito di membro del Consiglio di Istituto”.

- ✓ **Le scuole non possono usare il consenso degli interessati per trattare i dati**. La normativa sulla privacy impone alle pubbliche amministrazioni di agire con presupposti diversi dal consenso (attività istituzionale determinata dalle leggi e dai regolamenti e osservanza dell'interesse pubblico). È quanto precisato dal Garante della privacy nella motivazione dell'Ingiunzione n. 148 del 28 aprile 2022;
- ✓ Nel caso specifico il Garante si è occupato di un caso in cui una scuola ha mandato una comunicazione di posta elettronica mettendo in chiaro gli indirizzi e-mail di tutti i destinatari, facendo circolare sia gli stessi indirizzi sia implicitamente l'informazione relativa alla disabilità degli studenti, trattandosi di convocazione per gruppi di lavoro in materia di inclusione;
- ✓ La scuola, che ha ricevuto 1500 euro di sanzione, si è difesa sostenendo che l'istituzione scolastica sarebbe stata autorizzata dalle singole persone consenzienti rispetto all'utilizzo dell'indirizzo e-mail. Il Garante è stato di diversa opinione e ha sottolineato che il consenso non costituisce, di regola, un valido presupposto di liceità per il trattamento dei dati personali in ambito pubblico in ragione dello squilibrio della posizione degli interessati rispetto al titolare del trattamento.

VIOLA LAPRIVACY la pubblicazione sul sito istituzionale di determinazioni dirigenziali riguardanti aspetti organizzativi legati alla continuità della attività didattica e alla gestione del rapporto di lavoro

Provvedimento del 24 gennaio 2024 [9987578] - L'Autorità ha ricevuto un reclamo dalla sig.ra XX, docente in servizio presso l'Istituto Comprensivo Statale "F.S. Cabrini" (di seguito, "Istituto"), in ordine alla pubblicazione, sul sito istituzionale del predetto Istituto, di decine di determinazioni dirigenziali (circa trentasette) riguardanti aspetti organizzativi legati alla continuità della attività didattica e alla gestione del rapporto di lavoro con l'interessata, con particolare riferimento ai giorni di assenza dal servizio effettuati dalla reclamante e da altro personale scolastico e alla necessità di provvedere alla loro sostituzione nel corso dell'anno scolastico 2021/2022.

Concetti da ricordare:

La PA è tenuta a rispettare i principi indicati dal Regolamento europeo in materia di protezione dei dati personali (liceità, correttezza e trasparenza nonché di minimizzazione) e i dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati;

la Privacy deve guidare il processo di selezione dei dati personali da rendere o meno disponibili;

la finalità di rilevante interesse pubblico è la «realizzazione della Trasparenza pubblica» e non la pubblicazione nei siti istituzionali dei dati relativi agli interessati;

la previsione che «con la pubblicità siano rese note a tutti le informazioni, non comporta che tutte le informazioni debbano essere messe a disposizione del pubblico, cioè all'insieme dei destinatari»;

l'amministrazione deve essere una casa di vetro: ma i suoi abitanti devono comunque rimanere vestiti.

Inoltre ricordiamoci che la trasparenza delle informazioni chiama in causa anche le persone, ma:

non tutte le notizie che riguardano le persone coinvolte (sicuramente una larghissima fetta di popolazione, ma potenzialmente tutti i consociati) sono necessarie a soddisfare il bisogno della collettività di sapere come la macchina burocratica opera;
ci sono comunque categorie di informazioni che devono in ogni caso essere protette, poiché concernono strettamente, appunto, la dignità degli individui.

Privacy by design: in questa prospettiva – come affermato dal Garante - individuare strumenti di pubblicità rispettosi della privacy degli individui significa modellare in maniera soddisfacente il potere pubblico nell'equilibrio tra conoscenza (dell'attività) e riservatezza (delle persone)

Alcune regole essenziali:
Le Scuole sono tenute a porre in essere la massima attenzione nella selezione dei dati personali da utilizzare, sin dalla fase di redazione degli atti e documenti soggetti a pubblicazione, in particolare quando vengano in considerazione dati sensibili (in particolare, è necessario deindicizzare i dati sensibili e giudiziari)

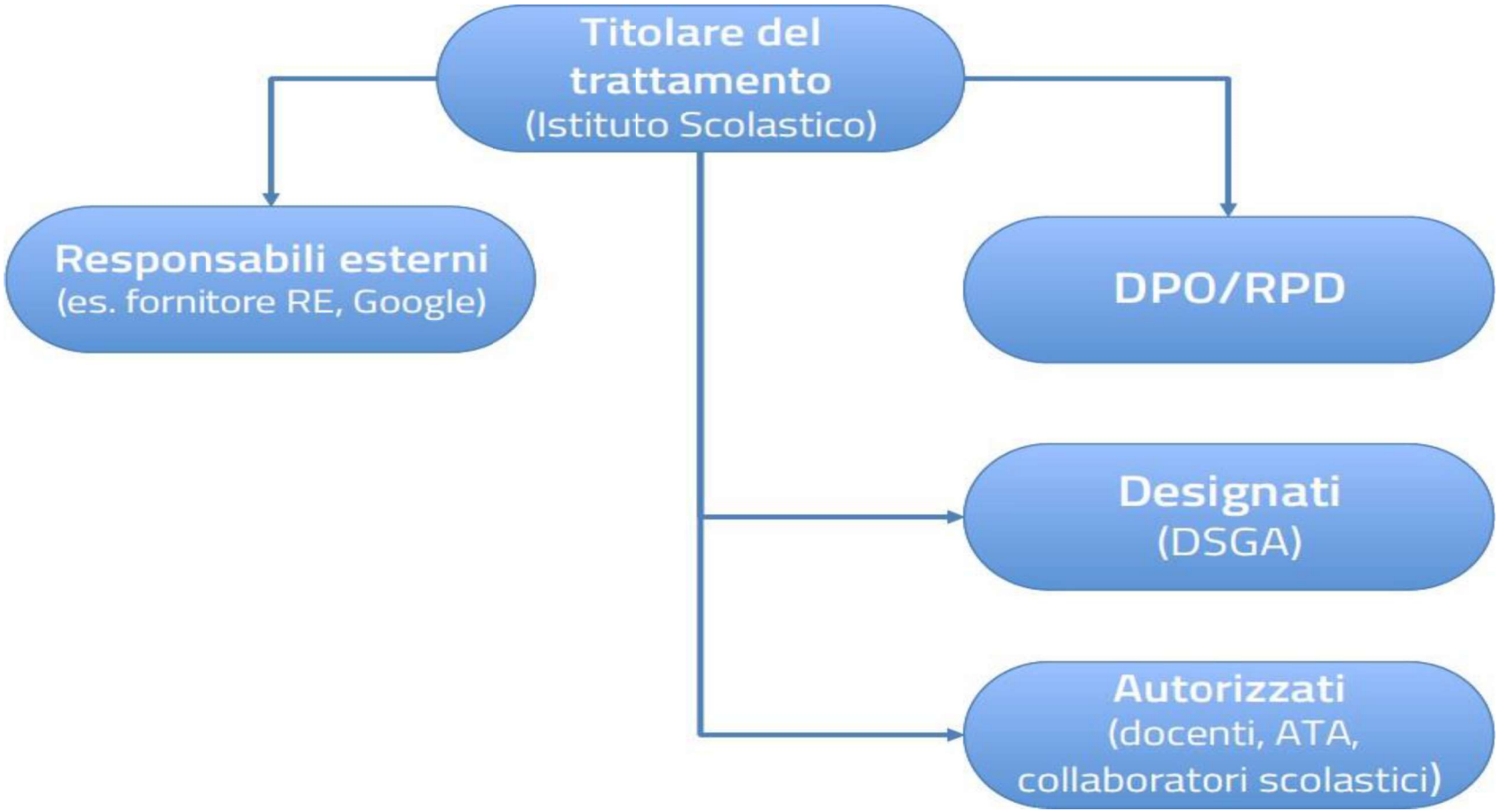
Può risultare utile non riportare queste informazioni nel testo dei provvedimenti pubblicati online (ad esempio nell'oggetto, nel contenuto, etc.), menzionandole solo negli atti a disposizione degli uffici (richiamati quale presupposto del provvedimento e consultabili solo da interessati e controinteressati)

L'eventuale pubblicazione di dati, informazioni e documenti, che non si ha l'obbligo di pubblicare, è legittima solo «procedendo alla anonimizzazione dei dati personali eventualmente presenti» (per anonimizzare un dato non è sufficiente sostituire il nome e cognome dell'interessato con le relative iniziali)

evitare che vengano resi ostensibili dati personali inutili a fini di trasparenza, ma che abbiano implicazioni afflittive sulla dignità degli interessati

IL REGOLAMENTO EUROPEO 2016/679 (GDPR)

I soggetti – organigramma privacy



Modifiche al codice di comportamento dei dipendenti della PA e le ricadute sull'organizzazione scolastica

- Il **DPR 81/23** ha apportato alcune integrazioni al **codice di comportamento per la PA** di cui al DPR 62/2013, per dare risposta alle nuove esigenze del contesto socio lavorativo e di quelle derivanti dalla evoluzione e diffusione dei social media anche nei contesti lavorativi.
- In particolare in relazione all'uso delle tecnologie viene integrato l'art. 11 bis (con cui si richiama all'utilizzo nelle comunicazioni con l'amministrazione di un account istituzionale, il divieto di usare quest'ultimo per altri fini) :

  2. L'utilizzo di account istituzionali è consentito per i soli fini connessi all'attività lavorativa o ad essa riconducibili e non può' in alcun modo compromettere la sicurezza o la reputazione dell'amministrazione. 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.

Modifiche al codice di comportamento dei dipendenti della PA e le ricadute sull'organizzazione scolastica

3. Il dipendente è responsabile del contenuto dei messaggi inviati. I dipendenti si uniformano alle modalità di firma dei messaggi di posta elettronica di servizio individuate dall'amministrazione di appartenenza. Ciascun messaggio in uscita deve consentire l'identificazione del dipendente mittente e deve indicare un recapito istituzionale al quale il medesimo è reperibile.

4. Al dipendente è consentito l'utilizzo degli strumenti informatici forniti dall'amministrazione per poter assolvere alle incombenze personali senza doversi allontanare dalla sede di servizio, purché' l'attività sia contenuta in tempi ristretti e senza alcun pregiudizio per i compiti istituzionali.

5. E' vietato l'invio di messaggi di posta elettronica, all'interno o all'esterno dell'amministrazione, che siano oltraggiosi, discriminatori o che possano essere in qualunque modo fonte di responsabilità dell'amministrazione.

Modifiche al codice di comportamento dei dipendenti della PA e le ricadute sull'organizzazione scolastica

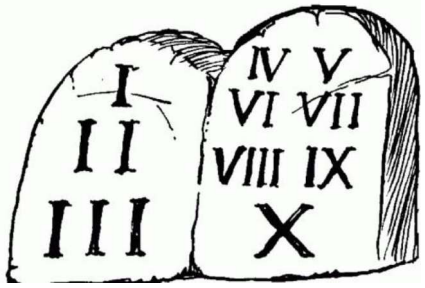
- **Utilizzo dei mezzi di informazione e dei social media**

- nell'utilizzo dei propri account di social media, il dipendente utilizza ogni cautela affinché le proprie opinioni o i propri giudizi su eventi, cose o persone, non siano in alcun modo attribuibili direttamente alla pubblica amministrazione di appartenenza;

- in ogni caso il dipendente è tenuto ad astenersi da qualsiasi intervento o commento che possa nuocere al prestigio, al decoro o all'immagine della Scuola;

- al fine di garantirne i necessari profili di riservatezza, le comunicazioni afferenti direttamente o indirettamente il servizio non si svolgono, di norma, attraverso conversazioni pubbliche mediante l'utilizzo di piattaforme digitali o social media.

Sono escluse da tale limitazione le attività o le comunicazioni per le quali l'utilizzo dei social media risponde ad una esigenza di carattere istituzionale.



I 10 COMANDAMENTI!

1) Ognuno è RESPONSABILE PERSONALMENTE
2) Ottenere il consenso per la pubblicazione di immagini/video
3) Non lasciare mai documenti con dati sensibili A VISTA
4) Conservare sempre registro e altri documenti in archivi con chiave
5) Evitare la diffusione di materiale e di informazioni su Whatsapp/Social
6) Predisporre informative per ogni nuovo iscritto/docente/fornitore… (entro 30gg)
7) Garantire il diritto all'oblio e/o alla non diffusione di dati
8) Per le comunicazioni elettroniche utilizzare SEMPRE canali crittografati
9) Comunicare tempestivamente ogni violazione
10) Analizzare sempre il rischio e progettare sempre misure idonee ad evitare la diffusione non autorizzata dei dati

Educazione alla privacy

La scuola ricopre anche un ruolo pedagogico:

- promuovere nei minori la consapevolezza dell'uso dei dati,
- educare alla cittadinanza digitale,
- sensibilizzare sull'uso corretto dei social,
- prevenire cyberbullismo, sexting, revenge porn.

Il trattamento dei dati personali può diventare occasione per formare cittadini digitali responsabili.

Il contesto scolastico è oggi fortemente digitalizzato: registro elettronico, comunicazioni scuola-famiglia via piattaforme digitali, uso di strumenti online per la didattica, gestione di documentazione sanitaria o di supporto (certificazioni, piani individualizzati, disabilità, BES/DSA), uso — sempre più frequente — di sistemi digitali e, recentemente, con l'introduzione di soluzioni basate su intelligenza artificiale (IA).

A ciò si aggiungono le esigenze di **trasparenza amministrativa**, imposte alle istituzioni scolastiche in quanto pubbliche amministrazioni, con obblighi di pubblicazione sul sito (attività, organigramma, dati di funzionamento, bandi, graduatorie, ecc.). Ciò determina una tensione tra esigenze di **trasparenza** e di **tutela della riservatezza/personale**, soprattutto quando si tratta di dati personali di studenti, famiglie, docenti, personale ATA.

Per questo motivo, la scuola deve contemperare con rigore i principi del Regolamento (UE) 2016/679 ("GDPR") e quelli degli obblighi di trasparenza amministrativa (es. D.Lgs. 33/2013 e successive delibere/linee guida in materia).

Le indicazioni del Garante Privacy, aggiornate al 2025, integrano il quadro normativo: non solo rafforzano misure di tutela dei dati personali, ma sottolineano la necessità di garantire trasparenza informativa e correttezza in tutte le fasi del trattamento

GDPR ISTRUZIONE

To Do List – **INFORMATIVE**

	Documento da personalizzare	Dove pubblicare
INF01	Informativa Alunni – Genitori - Tutori	Sito web sezione Privacy – Registro Elettronico
INF02	Informativa per il Personale (anche esterno)	Sito web sezione Privacy – Registro Elettronico
INF03	Informativa per i Fornitori	Sito web sezione Privacy – Atti con fornitori
INF07	Informativa sintetica	Firma posta – Contratti – Ogni documento con dati
INF04	Informativa Siti web	Sito web se non versione PNRR
INF06	Cookie Policy (TXT)(PDF)	Sito web se non versione PNRR
*	Informativa Google Workspace	Sito web sezione Privacy
*	Informativa Office 365	Sito web sezione Privacy
*	Informativa altre piattaforme utilizzate	Sito web sezione Privacy

* Da scaricare dal sito delle rispettive piattaforme

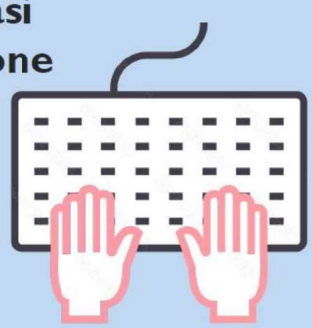
GDPR ISTRUZIONE

TRATTAMENTO dei DATI PERSONALI

Un TRATTAMENTO DI DATI PERSONALI è:

- la raccolta,
- la registrazione
- l'organizzazione
- la strutturazione
- la conservazione,
- l'adattamento o la modifica
- l'estrazione
- la consultazione
- l'uso
- la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione
- il raffronto o l'interconnessione
- la limitazione,
- la cancellazione o la distruzione

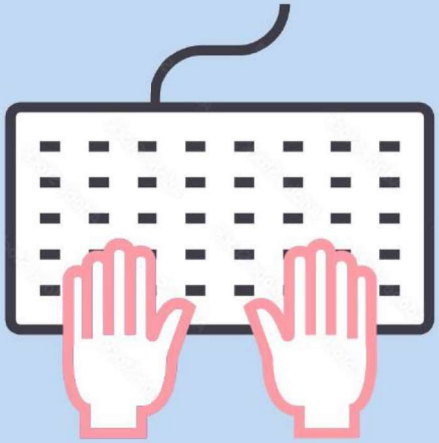
di dati personali.



Trattamento Dati nella Scuola

T1 - Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro:

- del **personale dipendente** dell'Amministrazione centrale e periferica del Ministero dell'istruzione, e dirigente, docente, educativo ed ATA e dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello Subordinato.
- Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.



Svolto da DS – DSGA – AA - RSU

Trattamento Dati nella Scuola

T2 - Gestione del contenzioso e procedimenti disciplinari:

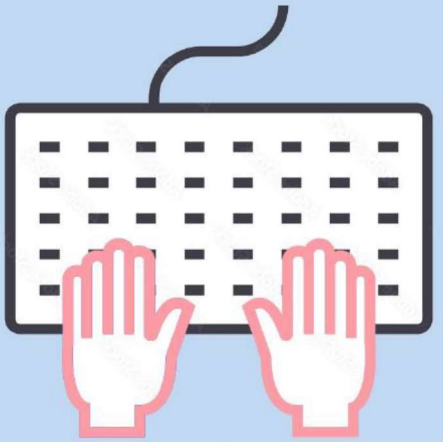
- Il trattamento dei dati concerne tutte le attività relative alla difesa in giudizio del Ministero dell'Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.

Svolto da DS – DSGA

Trattamento Dati nella Scuola

T3 - Organismi collegiali e commissioni istituzionali:

- Il trattamento dei dati necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali.



Svolto da DS – DSGA – AA – DOCENTE - CS

Trattamento Dati nella Scuola

T4 - Attività propedeutiche all'avvio dell'anno scolastico, ai corsi, e a tutte le attività formative:

- I dati sono forniti dagli **alunni**, dalle **famiglie**, dalle persone ai fini della frequenza dei corsi di studi nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

Svolto da DS – DSGA – AA – DOCENTE

Trattamento Dati nella Scuola

T5 - Attività educativa, didattica e formativa, e di valutazione:

- Il trattamento dei dati necessari all'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, valutazione periodica e finale, per le attività di orientamento e per la certificazione delle competenze..

Svolto da DS – DSGA – AA – DOCENTE - CS

Trattamento Dati nella Scuola

T7 - Rapporti scuola-famiglie-altri soggetti: gestione del contenzioso:

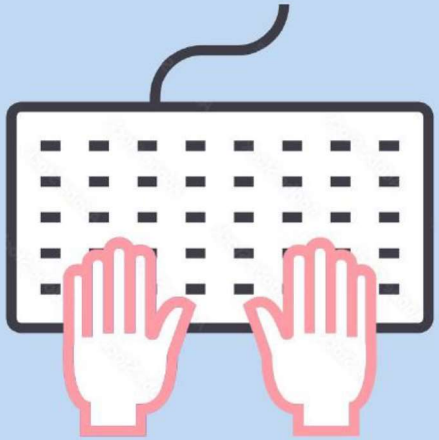
- Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di **contenzioso** (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce, all'autorità giudiziaria, etc.) con gli **alunni** e con le **famiglie**, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.

Svolto da DS – DSGA – AA – DOCENTE - CS

Trattamento Dati nella Scuola

T8 - Rapporti con i fornitori di beni e servizi:

- Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti di fornitura di beni e servizi, albo fornitori, gestione della rotazione, manifestazioni di interesse, e similari



Svolto da DS – DSGA – AA – (DOCENTE)

Trattamento Dati nella Scuola

T9 - Rapporti con enti e associazioni:

- Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti con enti pubblici, assimilati, e associazioni.

Svolto da DS – DSGA – AA – (DOCENTE)

Trattamento Dati nella Scuola

T10 - Videosorveglianza:

- Il trattamento dei dati concernenti le attività di gestione, conservazione dati, gestione degli accessi, ai sistemi di videosorveglianza.

Svolto da DS – DSGA – Incaricato Videosorveglianza

Trattamento Dati nella Scuola

- Schema TD

1	**Selezione e reclutamento a tempo indeterminato e determinato, e gestione del rapporto di lavoro,** del personale dipendente dell'Amministrazione centrale e periferica del Ministero dell'istruzione, e dirigente, docente, educativo ed ATA e dei collaboratori esterni e dei soggetti che intrattengono altri rapporti di lavoro diversi da quello Subordinato. *Il trattamento concerne tutti i dati relativi alle procedure per la selezione e il reclutamento, all'instaurazione, alla gestione e alla cessazione del rapporto di lavoro.*	X
2	**Gestione del contenzioso e procedimenti disciplinari** *Il trattamento dei dati concerne tutte le attività relative alla difesa in giudizio del Ministero dell'Istruzione e delle istituzioni scolastiche ed educative nel contenzioso del lavoro e amministrativo nonché quelle connesse alla gestione degli affari penali e civili.*	X
3	**Organismi collegiali e commissioni istituzionali** *Il trattamento dei dati necessario per attivare gli organismi collegiali e le commissioni istituzionali previsti dalle norme di organizzazione del Ministero Istruzione e dell'ordinamento scolastico. Tali organi sono rappresentativi sia del personale amministrativo e scolastico, sia degli studenti, delle famiglie e delle associazioni sindacali.*	X
4	**Attività propedeutiche all'avvio dell'anno scolastico, ai corsi, e a tutte le attività formative** *I dati sono forniti dagli alunni, dalle famiglie, dalle persone ai fini della frequenza dei corsi di studi nelle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.*	X

Trattamento Dati nella Scuola

- Schema TD

5	**Attività educativa, didattica e formativa, e di valutazione** *Il trattamento dei dati necessari all'espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, valutazione periodica e finale, per le attività di orientamento e per la certificazione delle competenze.*	X
6	Scuole non statali	
7	**Rapporti scuola-famiglie-altri soggetti: gestione del contenzioso** *Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di contenzioso (reclami, ricorsi, esposti, provvedimenti di tipo disciplinare, ispezioni, citazioni, denunce, all'autorità giudiziaria, etc.) con gli alunni e con le famiglie, e tutte le attività relative alla difesa in giudizio delle istituzioni scolastiche di ogni ordine e grado, ivi compresi convitti, educandati e scuole speciali.*	X
8	**Rapporti con i fornitori di beni e servizi** *Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti di fornitura di beni e servizi, albo fornitori, gestione della rotazione, manifestazioni di interesse, e similari*	X
9	**Rapporti con enti e associazioni** *Il trattamento dei dati concernenti tutte le attività connesse alla instaurazione di rapporti con enti pubblici, assimilati, e associazioni*	X
10	**Video Sorveglianza** *Il trattamento dei dati concernenti le attività di gestione, conservazione dati, gestione degli accessi, ai sistemi di videosorveglianza*	X

To Do List – **AUTORIZZAZIONI** (NOMINE)

	Documento da personalizzare	Come gestire
LN01	Lettera di Autorizzazione (nomina) DSGA	Completare e far sottoscrivere al personale volendo anche con FEA (Sigillo SIDI) Se si ritiene opportuno protocollare Inserire nel fascicolo Autorizzazioni Privacy Inserire nel fascicolo del dipendente
LN03	Lettera di Autorizzazione (nomina) Docenti, Supplenti, Formatori esterni	
LN03B	Lettera di Autorizzazione (nomina) Tirocinanti	
LN04-1	Lettera di Autorizzazione (nomina) Assistenti Amministrativi	
LN05	Lettera di Autorizzazione (nomina) Assistenti Tecnici	
LN06-1	Lettera di Autorizzazione (nomina) Collaboratori Scolastici	

To Do List – **Responsabili Esterni**

	Documento da personalizzare	Come gestire
LN07	Lettera di Autorizzazione (nomina) Amministratore di Sistema	Completare e far sottoscrivere ai Responsabili Esterni Protocollare Inserire nel fascicolo Responsabili Privacy
LN13	Nomina ditta Assistenza Informatica	
LN13	Nomina Ditta Fotocopiatrici	
*	Nomina Ditta Registro Elettronico	
*	Nomina Ditta Segreteria Digitale	
*	Nomina Ditta altri servizi di Responsabili Esterni	

* In genere fornita dalle aziende delle rispettive piattaforme

All’inizio dell’anno scolastico nascono spontaneamente gruppi WhatsApp nelle classi.

- Obiettivo iniziale: coordinamento didattico e organizzativo.
- Rischio: confusione e sovraccarico informativo.

I gruppi WhatsApp si formano con l'intento di facilitare il coordinamento per materiali didattici, orari e attività extrascolastiche, ma, questi canali di comunicazione non ufficiali rischiano di trasformarsi in fonti di confusione e **rumore informativo**.

Rischi operativi

Flusso eccessivo di notifiche

- Condivisione non necessaria di foto e informazioni.
- Sostituzione impropria degli strumenti ufficiali e/o comunicazioni scuola–famiglia.

Rischi operativi

Durante le prime settimane di scuola, il flusso incessante di notifiche genera spesso più problemi di quanti ne risolva: richieste continue sui compiti, su cosa studiare, condivisioni massive di foto dei quaderni e promemoria ripetitivi creano un circuito parallelo che può sostituire impropriamente l'autonomia degli studenti e gli **strumenti ufficiali** di comunicazione scuola-famiglia.

Gruppi WhatsApp ≠ canale istituzionale

Non sostituiscono registro elettronico o le comunicazioni ufficiali.

Se presenti figure scolastiche, aumentano responsabilità e obblighi.

Privacy e tutela dei minori

Dati personali e immagini devono essere trattati con cautela.

- Condivisione solo di informazioni necessarie.
- Rispetto degli orari e della riservatezza.

Netiquette consigliata

Messaggi sintetici e pertinenti.

- No giudizi su docenti o alunni.
- Chat solo per promemoria logistici.

Uso responsabile

Evitare catene e inoltri.

- Libertà di silenziare o uscire dal gruppo.
- Temi delicati da gestire tramite colloqui formali.

La sentenza della **Corte di Cassazione** n. 29683/2025 pone all'attenzione questioni ancora più delicate, trasformando l'uso improprio di questi strumenti da semplice maleducazione digitale a potenziale **reato**.

Sentenza Cassazione n. 29683/2025

Pubblicazione non autorizzata della foto profilo = reato.

- Rilevanza maggiore quando coinvolge minori.

Protocollo Privacy per le Istituzioni Scolastiche

1. Premessa e Finalità

- Il presente Protocollo definisce regole, responsabilità e procedure per il trattamento dei dati personali nell'istituzione scolastica, in conformità al GDPR, alla normativa nazionale vigente, alle Linee guida del Garante della Privacy 2025 e agli obblighi di trasparenza previsti dal D.Lgs. 33/2013.

2. Ambito di Applicazione e Soggetti Coinvolti

- Il Protocollo si applica a tutti i trattamenti di dati personali, in qualsiasi forma e formato, effettuati dalla scuola. Sono coinvolti: Titolare del trattamento, DPO, responsabili e incaricati, fornitori esterni e terzi autorizzati.

3. Principi Generali di Trattamento

- Liceità, correttezza, trasparenza; limitazione delle finalità; minimizzazione; esattezza; limitazione della conservazione; integrità e riservatezza.

4. Governance: Ruoli e Responsabilità

- Descrizione dei compiti del Dirigente scolastico, DPO, responsabili e incaricati del trattamento, fornitori esterni.

5. Strumenti Documentali e Registrazioni

- Registro dei trattamenti, nomine e deleghe, informative e moduli di consenso, policy interne, regolamentazioni d'uso degli strumenti digitali.

6. Aree di Trattamento e Modalità Operative

- - Dati amministrativi e didattici
- - Dati sensibili e particolari
- - Immagini, foto, video e materiale audiovisivo
- - Comunicazioni scuola-famiglia
- - Uso di tecnologie digitali e Intelligenza Artificiale
- - Pubblicazione atti e obblighi di trasparenza

Protocollo Privacy per le Istituzioni Scolastiche

7. Gestione Data Breach e Diritti degli Interessati

- Procedure per segnalazione, valutazione e comunicazione delle violazioni; esercizio dei diritti.

8. Formazione e Sensibilizzazione

- Percorsi formativi periodici per il personale; informazione a studenti e famiglie; audit interni.

9. Pubblicazione Contenuti Online e Social

- Policy di autorizzazione e pubblicazione; obbligo di valutazione preventiva e anonimizzazione.

10. Procedure e Modulistica

- Esempi: registro trattamenti, lettere di nomina, informative, liberatorie foto/video, moduli diritti, DPIA, policy IT.

11. Aggiornamento e Revisione del Protocollo

- Revisione periodica, approvazione del Dirigente, comunicazione al personale, pubblicazione nella sezione dedicata del sito.

12. Conformità alle Linee Guida 2025 del Garante

- Prescrizioni su IA, minimizzazione dati, valutazioni di impatto, divieto di pratiche invasive.

13. Schema di Governance e Controllo Interno

- Nomina DPO, comitato privacy, audit periodici, monitoraggio e registro revisioni.

14. Conclusioni

- Il Protocollo garantisce tutela dei diritti, trasparenza amministrativa e corretto uso delle tecnologie, incluse IA, nel rispetto della normativa.

Privacy e responsabilità: quando il gruppo non sostituisce l’istituzione

La natura privata dei **gruppi WhatsApp** rappresenta un aspetto cruciale da considerare. Non costituendo canali istituzionali, non possono in alcun modo sostituire il **registro elettronico**, le circolari o le comunicazioni ufficiali della **dirigenza scolastica**. La situazione cambia quando vi partecipano figure del **personale scolastico**: in questo caso, le responsabilità si amplificano e diventa necessario stabilire chiarezza su finalità, partecipanti e modalità di gestione dei dati.

La **privacy dei minori** richiede particolare attenzione: numeri personali, immagini e **informazioni sensibili** devono essere trattati con estrema parsimonia, rispettando i confini orari e limitando la diffusione esclusivamente a contenuti strettamente necessari per la vita della classe. L'adozione di una **netiquette condivisa** può trasformare questi strumenti in risorse utili anziché fonte di stress: messaggi sintetici e pertinenti, rispetto di orari ragionevoli, divieto assoluto di giudizi su docenti o compagni rappresentano i pilastri di un protocollo di buon senso.

Le questioni delicate devono essere rimandate ai **colloqui formali**, mentre le chat dovrebbero limitarsi a promemoria logistici senza trasformarsi in arena di dibattiti. Il divieto di inoltri e catene, l'attenzione nella condivisione di foto e la libertà di silenziare o abbandonare il gruppo senza stigmatizzazioni completano il quadro di un uso responsabile.

Raccomandazione del Garante nazionale delle persone con disabilità n. 1/2025 - accesso alla classe da parte di professionisti sanitari.

Il decreto legislativo 5 febbraio 2024, n. 20, emanato in attuazione della delega contenuta nella legge n. 227/2021, ha istituito l'Autorità denominata "Garante nazionale dei diritti delle persone con disabilità", con il compito di assicurare la piena attuazione e la tutela dei diritti e degli interessi delle persone con disabilità. A tale Autorità sono attribuite funzioni e prerogative di vigilanza sul rispetto dei diritti delle persone con disabilità e sulla conformità dell'azione amministrativa ai principi sanciti dai trattati internazionali, dal diritto dell'Unione europea e dalla normativa nazionale. L'Autorità esercita, inoltre, attività di contrasto a ogni forma di discriminazione e di promozione dell'effettivo godimento dei diritti e delle libertà fondamentali delle persone con disabilità.

Raccomandazione del Garante nazionale delle persone con disabilità n. 1/2025 - accesso alla classe da parte di professionisti sanitari.

l'Autorità Garante nazionale dei diritti delle persone con disabilità ha formulato la raccomandazione n. 1/2025 del 23 ottobre 2025, che si allega alla presente per opportuna conoscenza, avente ad oggetto: "accesso alla classe da parte di professionisti sanitari - raccomandazione ai sensi dell'art. 4, comma1 lett. g) del d. lgs.n.20/2024".

Raccomandazione del Garante nazionale delle persone con disabilità n. 1/2025 - accesso alla classe da parte di professionisti sanitari.

raccomandazione:

-nelle ipotesi di accesso di professionisti sanitari esterni incaricati (dipendenti della ASL, di ente/struttura accreditata e/o autorizzata presso il SSN/SSR, ovvero iscritti ai rispettivi albi professionali e coinvolti nel piano terapeutico, riabilitativo, assistenziale o nel progetto di vita dell'alunno con disabilità), necessari per l'attuazione del progetto personalizzato in favore di alunni e studenti con disabilità, deve essere rilasciata esclusivamente l'autorizzazione del Dirigente Scolastico, previa comunicazione del predetto accesso ai docenti e ai genitori degli altri alunni della classe interessata e previa dichiarazione dello specialista in ordine al rispetto di tutte le disposizioni in materia di riservatezza, con l'impegno a non interagire direttamente con gli alunni non interessati e a permanere nella classe sempre in presenza del docente.

Raccomandazione del Garante nazionale delle persone con disabilità n. 1/2025 - accesso alla classe da parte di professionisti sanitari.

raccomandazione:

Alla luce di quanto sopra, si sollecita la modifica di qualsivoglia regolamento d'istituto che preveda una procedura differente rispetto alla suddetta raccomandazione, ivi compresa la richiesta del consenso dei docenti e dei genitori degli altri studenti a permettere l'ingresso in classe del professionista esterno, non potendo tale ingresso essere sottoposto, e quindi limitato, ritardato ovvero negato, in caso di mancato consenso da parte anche di uno solo dei soggetti coinvolti.

Al fine di assicurare la tutela effettiva dei diritti costituzionalmente garantiti di tutti gli studenti interessati ed uniformità di condotta su tutto il territorio nazionale, si chiede di assicurare la massima diffusione della presente raccomandazione presso tutte le istituzioni scolastiche, di ogni ordine e grado, pubbliche, paritarie e private".

… ma cosa genera una vulnerabilità

Era davvero necessaria?

ERRORE TIPICO: obiettare che non si ha nulla da nascondere.

E se i dati che non nascondiamo passassero di mano in mano e fossero male interpretati?

ESEMPIO: CARD NOMINATIVE DEI SUPERMERCATI

minimarket familiare → catene supermercati → fondi di investimenti

RISULTATO:
Miei comportamenti si potrebbero riflettere nelle richieste di mutui/servizi assicurativi
Non è fantascienza: In UK è successo proprio questo alle catene di PUB

Negligenti con le nostre mail?

Mia mail

tutti i documenti che sono transitati negli anni dalla mail:

- CI / CF
- estratti conto bancari (IBAN / ecc)
- conti telefonici e numeri di SIM

POTENZIALE FURTO DELLA MIA IDENTITA', CLONAZIONI SIM, ALTRO

- **ricatti**
- **furti di account più importanti**
- **ecc.**

Errore tipico che genera vulnerabilità

Secondo Esempio :
REGISTRAZIONE NEI VARI SITI UTILIZZANDO SEMPRE LA STESSA MAIL

Mia mail

renato.narcisi@netsenseweb.com
password123

1 **iscrizione a vari siti**

renato.narcisi@netsenseweb.com
password123

renato.narcisi@netsenseweb.com
differentePassword

renato.narcisi@netsenseweb.com
altraPassword

2 **siti brecciati**

3

BINGO!!! (si fa per dire)
una delle tre credenziali corrisponde
sono entrati nella mia mail…..

renato.narcisi@netsenseweb.com / differentePassword
renato.narcisi@netsenseweb.com / password123
renato.narcisi@netsenseweb.com / altraPassword

COSA FARE?

- Cambiare password nella propria mail.

- Utilizzare una mail SOLO per le cose importanti e una seconda per le altre

MA SOPRATTUTTO:
Imparare che la password è importante quanto le chiavi di un oggetto materiale.

La responsabilità di furti di dati / perdita di privacy /ecc. ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

MISURE CAUTELA : PASSWORD

CHIARO RIFERIMENTO: (Gestionali e Registro Elettronico)

Perché rispettare le prescrizioni del Codice nella scelta delle password?

Se qualcuno accede ad un computer o ad un servizio WEB potrà impossessarsi di dati personali e aziendali.

La responsabilità di questa sottrazione ricadrà sull'addetto al trattamento, se il dispositivo non era protetto da password, o se la password era troppo debole.

Il 90% dei furti di identità sono riconducibili ad un uso non responsabile delle password

La password

Suggerimenti per creare una password sicura (tratto dal sito della polizia postale):

- Creare una password di minimo dieci caratteri, contenente almeno una maiuscola, almeno una minuscola, almeno un numero e almeno un carattere speciale tra quelli elencati: ! $? # = * + - . , ; :
- Includere caratteri dall'apparenza simili in sostituzione di altri caratteri (ad esempio il numero “0” per la lettera “O” o il carattere “$” per la lettera “S”).
- Creare un acronimo univoco (ad esempio "PDRM" per "Piazza Delle Repubbliche Marinare").

Includere sostituzioni fonetiche o grafiche (ad esempio “6 arrivato” per “Sei arrivato” o “Arrivo + tardi” per “Arrivo più tardi”).

Da evitare:

- Non utilizzare le stesse password per più account.
- Non usare una password già utilizzata in un esempio di come si sceglie una buona password.
- Non utilizzare una password contenente dati personali (nome, data di nascita, ecc.).
- Non usare parole o acronimi che si possono trovare nel dizionario.
- Non usare sequenze di tasti sulla tastiera (asdf) o sequenze di numeri (1234).
- Non creare password di soli numeri, di sole lettere maiuscole o di sole lettere minuscole.
- Non usare ripetizioni di caratteri (aa11).

Suggerimenti per tenere al sicuro la password:

- Non comunicare a nessuno la password (inclusi partner, compagni di appartamento, colleghi, ecc.).
- Non lasciare la password scritta in posti facilmente raggiungibili da altri.
- Non inviare mai la password per email.
- Verificare periodicamente la password corrente e cambiarla con una nuova.

I trattamento dei dati cartacei

ATTENZIONE alla carta riciclata!

ATTENZIONE alle stampe che si lasciano!

Se la stampante è condivisa con altri utenti o è fuori dal campo visivo evitare di lasciare le stampe per troppo tempo, perché degli utenti non autorizzati potrebbero visualizzarle o asportarle.

Ransomware cos'è?

Il ransomware è un programma informatico dannoso che infetta un dispositivo (PC, Tablet, Smartphone, Smart TV), bloccando l'accesso ai contenuti (foto, video, file) e chiedendo un riscatto (ransom) per «liberarli».

La richiesta di pagamento con le relative istruzioni è presentata in una finestra che appare automaticamente sullo schermo del dispositivo infettato.
L'utente ha pochi giorni per pagare, poi il blocco dei file diventa definitivo.

Ci sono 2 tipi principali di ransomware:
Cryptor: criptano i file contenuti nel dispositivo rendendoli illeggibili;
Blocker: bloccano l'accesso al dispositivo infettato.

Ransomware come si diffonde?

Il ransomware si diffonde soprattutto attraverso messaggi inviati via e-mail, sms o chat o che appaiono su pagine web e social network, che sembrano provenire da soggetti conosciuti e sicuri (corrieri espressi, gestori di servizi (acqua, luce, gas), operatori telefonici, soggetti istituzionali ecc.

Chi li riceve è indotto ingannevolmente ad aprire allegati o a cliccare link o banner collegati a software dannosi.

Il dispositivo infettato può a sua volta «contagiarne» altri, perché il ransomware, impossessandosi della rubrica dei contatti, può utilizzarla per spedire automaticamente messaggi contenenti file dannosi.

Ransomware come difendersi?

La prima difesa dai ransomware è **evitare di aprire messaggi provenienti da soggetti sconosciuti** o con i quali non si hanno rapporti (ad es. un operatore telefonico di cui non si è cliente, un corriere da cui non si aspettano consegne, ecc.) e non cliccare su collegamenti a siti sospetti.

E' utile installare un **antivirus con estensione per malware** sui propri dispositivi e mantenere aggiornato il sistema operativo.

E' fondamentale **effettuare backup periodici dei contenuti**, così, nel caso in cui fosse necessario formattare il dispositivo per sbloccarlo, i dati in esso contenuti non verranno persi.

Ransomware come liberarsene?

Pagare il riscatto è solo apparentemente la soluzione più facile. Oltre al danno economico, si corre infatti il rischio di non ricevere i codici di sblocco, o addirittura di finire in liste di «pagatori», potenzialmente soggetti a periodici attacchi ransomware. L'alternativa è quella di rivolgersi a tecnici specializzati capaci di sbloccare il dispositivo.
Oppure si può formattare il dispositivo, ovviamente se si ha a disposizione un backup. E' consigliabile sempre segnalare o denunciare l'attacco ransomware alla Polizia Postale, anche per aiutare a prevenire ulteriori truffe.

“Il problema non é fare la cosa giusta … ma sapere qual é la cosa giusta”
Lyndon B. Johnson

Grazie dell’attenzione!!!

Domande, istanze, interpellanze, dubbi, perplessità!