

G	D	P	R	-	G	E	N
E	R	A	L		D	A	T
A		P	R	O	T	E	C
T	I	O	N		R	E	G
U	L	A	T	I	O	N	



Finalità del GDPR

Fare in modo che i dati che sono in possesso dell' Istituto Scolastico seguano le regole principali della Privacy e cioè:

Finalità del GDPR

I dati siano raccolti in modo legale

Basi GIURIDICHE del TRATTAMENTO

1. Consenso
2. Adempimento obblighi contrattuali
3. Obblighi di legge del Titolare
4. Interessi vitali Interessato
5. Legittimo interesse Titolare o terzi
6. Interesse pubblico o esercizio pubblici poteri

Art. 6 GDPR

Finalità del GDPR

I dati seguano l'iter previsto

1. Siano trattati da chi ne ha il diritto (Siano VISIBILI e MODIFICABILI da soggetti specificati)
2. Vadano COMUNICATI alle persone giuste
3. Il loro trattamento non arrechi danno agli interessati

Finalità del GDPR

Siano necessari e
sufficienti

Finalità del GDPR

**Il loro uso sia
trasparente per gli
interessati**

Finalità del GDPR

Vengano DISTRUTTI
quando non più utili

Finalità del GDPR

Per fare questo
occorre definire
FIGURE e TRATTAMENTI

Attori



Interessato

Persona fisica identificata o identificabile.

Si considera identificabile la persona fisica che può essere riconosciuta, direttamente o indirettamente, con particolare riferimento a un dettaglio come il nome, un numero di documento, dati relativi all'ubicazione, un dato riferito a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale



Attori



un dato
riferito a uno
o più
elementi
caratteristici
della sua
identità
fisica

Attori



Titolare del trattamento

Persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo che, singolarmente o insieme ad altri, **determina le finalità e i mezzi del trattamento di dati personali;**

Quindi è colui che decide quali dati raccogliere, come trattarli, quanto tempo e come conservarli, a chi vanno comunicati, quali rischi comportano.



Attori



Data Protection Officer

- **Obbligatorio** per P.A.
- **Obbligatorio** per titolari di trattamenti di dati in grande scala
- **Obbligatorio** per titolari di trattamenti di dati sensibili (particolari)

Figura di riferimento per PA, imprese, utenti, clienti ed **interfaccia** con autorità garante

Attori



Responsabile del trattamento



Persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo **che tratta dati personali per conto del titolare** del trattamento. Quindi non è colui che decide quali dati usare, ma quali sono i metodi o gli incaricati più adatti per portare a termine le direttive del Titolare, quali sono i dati particolari e quali i rischi.
È abilitato a modificare i dati.

Attori



SUB-Responsabile del trattamento



Persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo indicato dal Responsabile del trattamento.

Tratta i dati su specifiche del Responsabile.

È abilitato a modificare i dati.



Attori



Autorizzato al trattamento



Nel par.4 punto 10 si accenna a questa figura. È detto «persona sotto il controllo del titolare». Anche nella vers. Inglese il termine è «persons». Quindi non è chiaro se sono **solo** pers. Fisiche.

Quindi **segue le regole** che gli vengono consegnate dal Titolare e dal Responsabile del trattamento, **senza influire** sul tipo di dato e sul trattamento stesso.

Attori



Destinatario del trattamento

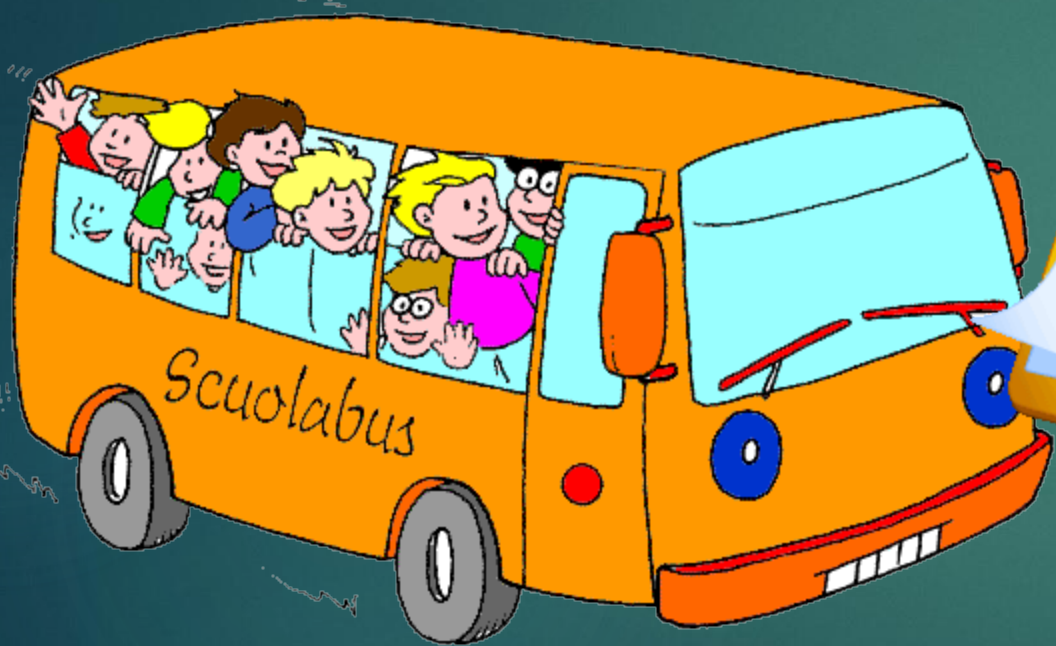
Persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo **che riceve prevista comunicazione di dati personali** (trattati o no).
In questo caso, il dato viene «**comunicato**».



Attori



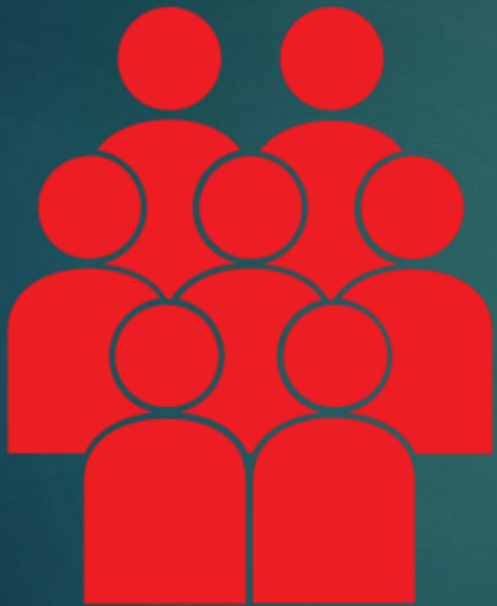
Destinatario del trattamento



Attori



Terzo



Chiunque (persona fisica o giuridica, l'autorità pubblica, servizio o altro organismo) riceva prevista o imprevista comunicazione di dati, che **non sia** o l'interessato o il titolare del trattamento o responsabile del trattamento o destinatario o persona autorizzata al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

Un dato, se comunicato a terzi, viene detto «**diffuso**»

Attori



Autorità di controllo

Ogni Stato dell'Unione europea ha la sua **Autorità di controllo**, che è pubblica, indipendente e competente per la gestione dei reclami ad essa proposti o di eventuali violazioni del REGOLAMENTO EUROPEO.

Il **Garante per la protezione dei dati personali** (Garante Privacy) è l'**autorità di controllo nazionale italiana**. La sua sede è a Piazza di Monte Citorio n. 121 in Roma



Accountability

Primo passo alla conformità (compliance): sapere capire e designare chi gestisce i dati

Dato personale identificativo

Qualsiasi dato che identifica univocamente una persona fisica

Data protection impact assessment (DPIA)

Il modo di identificare i rischi nei metodi usati per trattare i dati

Diritto all' oblio

Diritto dell' interessato di richiedere la cancellazione da qualsiasi lista. Se la richiesta ne implica la totale cancellazione, è un problema. Non ancora chiarito.

Dato personale

Dato relativo ad una persona fisica (nome, documento, domicilio, id. online o fattori fisici, psicologici, genetici, mentali, economici, culturali, sociali)

Persona fisica

In termini legali, un essere umano

Consenso

Indicazione non ambigua o azione positiva data dall' interessato in forma verbale o scritta ai fini del trattamento dei propri dati personali

Data Protection Officer (DPO)

Persona fisica o giuridica con responsabilità di supportare il Titolare, il Responsabile al trattam. e gli incaricati

Diritto di accesso ai dati

Diritto dell' interessato a chiedere al Titolare gratuitamente i propri dati personali

Responsabile trattam. dati

Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento

Persona giuridica

A differenza della fisica, è un individuo, un organismo o altra entità che ha diritti legali

Data breach

Questo è ciò che il GDPR si prefigge di evitare: quando la sicurezza dei dati di una persona fisica è compromessa o esposta.

Interesse legittimo

Un' area molto grigia, in cui il Titolare decide autonomamente se trattare un dato

Diritto ad essere informati

Diritto dell' interessato di ricevere chiara informazione sul presente, futuro o possibile trattam. dati

Profilazione

Analizzare gli interessi, preferenze, comportamenti, posizioni e movimenti di una persona fisica

Interessato

Persona fisica alla quale si riferiscono i dati personali

Titolare del trattamento

Persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che determina gli scopi e le modalità della raccolta dei dati

Trattamento

Qualsiasi uso si faccia dei dati personali (es. raccolta, strutturazione, registrazione, analisi).

Diritto alla limitazione del trattamento

Diritto dell' interessato di sospendere il trattamento. Non implica cancellazione.

Dato particolare (sensibile)

Dati che indicano provenienza etnica, opinioni politiche, credo religioso o filosofico, sindacato, genetica, biometrica, salute, vita e orientamento sessuale

SCUOLA

Importanza della Privacy

COME AFFERMATO ANCHE DAL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI «L'ISTRUZIONE RAPPRESENTA UNA RISORSA FONDAMENTALE PER OGNI PAESE perché CONIUGA MEMORIA STORICA E FUTURO»

PER QUESTA RAGIONE È CERTAMENTE IMPORTANTE ESSERE SEMPRE AL PASSO CON L'INNOVAZIONE MA ANCOR PIÙ IMPORTANTE È AFFERMARE, ANCHE ATTRAVERSO L'ESEMPIO, **I PRINCIPI DI CIVILTÀ, RISERVATEZZA E DIGNITÀ DELLA PERSONA**

SCUOLA

BASI GIURIDICHE (ART. 6 CONDIZIONI DI LICEITÀ)

il trattamento dei dati personali è lecito solo se basato su una delle seguenti condizioni di liceità:

- **consenso** (nella scuola pubblica non serve per le finalità istituzionali)
- **esecuzione di un contratto** in cui l'interessato è parte
- **adempimenti ad obblighi di legge** cui è soggetto il titolare
- salvaguardia degli interessi **vitali** dell'interessato
- esecuzione di un compito di **interesse pubblico**
- interesse **legittimo** del titolare (purchè non prevalga sui diritti fondamentali dell'interessato)

SCUOLA

CONSENSO

Qualsiasi manifestazione di volontà **libera, specifica, informata, inequivocabile** dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano **siano oggetto di trattamento**.

Il consenso dell'interessato può essere formulato, ad esempio, mediante dichiarazione scritta, anche attraverso mezzi elettronici, o verbalmente. Questo può avvenire anche con la selezione di una apposita casella di un sito web.

NON È CONSENSO IL SILENZIO ASSENSO, L'INATTIVITÀ O LA PRESELEZIONE DI CASELLE.

Il consenso è sempre revocabile.

SCUOLA

I DIRITTI

DI INFORMAZIONE ----->

INFORMATIVA sia CONCISA, CHIARA, ACCESSIBILE

DI ACCESSO ----->

VERIFICA PROPRI DATI E RELATIVI TRATTAMENTI

ci si può rivolgere al titolare e se non si ottiene risposta è possibile rivolgersi direttamente al garante o alla magistratura ordinaria.

diverso è l'accesso agli atti di cui alla legge 241/1990 (necessità di interesse diretto, concreto e attuale) e accesso civico di cui al d. l.gsl. 33/2013 modificato con d. lgs 97/2016

DI RETTIFICA ----->

POSSIBILITÀ DI MODIFICA DEI PROPRI DATI

DI CANCELLAZIONE (OBLIO) ----->

REVOCA DEL CONSENSO E CANCELLAZIONE

DI LIMITAZIONE ----->

CORREZ. INESATTEZZE E LIMITAZIONE TRATT.

PORTABILITÀ DEI DATI ----->

TRASFERIMENTO DATI AD ALTRO TITOLARE

DI OPPOSIZIONE ----->

OPPOSIZIONE IN OGNI MOMENTO AL TRATT.

SCUOLA

IL PRINCIPIO DI ACCOUNTABILITY

ART. 5 COMMA 2: IL TITOLARE È COMPETENTE DEL RISPETTO DEL PARAGRAFO 1 (PRINCIPÌI) ED È IN GRADO DI COMPROVARLO.

CONSIDERANDO 74: IL TITOLARE DEL TRATTAMENTO DOVREBBE ESSERE TENUTO A METTERE IN ATTO MISURE ADEGUATE ED EFFICACI ED ESSERE IN GRADO DI DIMOSTRARE LA CONFORMITÀ DELLE ATTIVITÀ DI TRATTAMENTO CON IL PRESENTE REGOLAMENTO, COMPRESA L'EFFICACIA DELLE MISURE. TALI MISURE DOVREBBERO TENER CONTO DELLA NATURA, DELL'AMBITO DI APPLICAZIONE, DEL CONTESTO E DELLE FINALITÀ DEL TRATTAMENTO, nonché DEL RISCHIO PER I DIRITTI E LE LIBERTÀ DELLE PERSONE FISICHE.

*ART. 24: IL TITOLARE DEVE ESSERE IN GRADO DI DIMOSTRARE CHE IL TRATTAMENTO È CONFORME AL **REGOLAMENTO**.*

Il titolare ha quindi l'obbligo di dimostrare la «compliance» anche mediante l'adozione di politiche interne e meccanismi per garantire IL rispetto DEL G.D.P.R. - attuazione del principio di protezione dei dati BY DESIGN E BY DEFAULT

In virtù del principio di accountability (responsabilizzazione), ogni titolare deve adottare criteri e comportamenti tali da dimostrare la corretta adozione di misure analizzate ad assicurare l'applicazione del regolamento in materia di protezione dei dati personali. Il titolare del trattamento effettua un processo di valutazione delle misure tecnico/organizzative che deve adottare per mitigare i rischi connessi al trattamento dei dati

SCUOLA

L'accountability in concreto

Adeguare al REGOLAMENTO un'organizzazione implica un **sistema di gestione della privacy** INTESA COME insieme di procedure, documenti, regole e dispositivi di controllo anche tra loro integrati ed informatizzati, modellato per adattarsi all'evoluzione della normativa e dell'organizzazione, strutturato per favorire il miglioramento continuo Integrato con gli altri processi amministrativi e didattici

Un corretto sistema di gestione, implica:

- LA VERIFICA DELLE INFORMATIVE
- L'INDIVIDUAZIONE E NOMINA RESPONSABILI
- L'INDIVIDUAZIONI E ISTRUZIONI AGLI AUTORIZZATI
- IL REGISTRO DEI TRATTAMENTI
- L'ANALISI DEI RISCHI E MISURE DI SICUREZZA
- LA VALUTAZIONE DI IMPATTO (PIA) (se necessaria)
- IL CONTROLLO DI CONSERVAZIONE DELLA DOCUMENTAZIONE
- UNA PROCEDURA DI DATA BREACH
- LA NOMINA DEL Data Protection Officer (NECESSARIA per amm.pubbliche)
- Audit, aggiornamento e formazione

SCUOLA

LA COMPLIANCE PARTE DA OGNUNO DI NOI

ESSERE **COMPLIANT** NON SIGNIFICA SEMPLICEMENTE ADOTTARE UN MODELLO DI GESTIONE.

LA VERA COMPLIANCE PARTE DA OGNI SINGOLO OPERATORE CHE, NELL'AMBITO DELLA SUA MANSIONE, DEVE PORRE IN ESSERE COMPORTAMENTI CHE DIMOSTRINO LA CONOSCENZA DEI PRINCIPI E DEI DIRITTI CHE LA NORMATIVA PRIVACY GARANTISCE.

SIGNIFICA CERTO SAPERE CHE L'ISTITUTO SCOLASTICO HA ADOTTATO UN MODELLO DI GESTIONE, MA SOPRATTUTTO SIGNIFICA CONOSCERE IL **PROPRIO RUOLO ALL'INTERNO DELL'ORGANIGRAMMA PRIVACY** E PORRE IN ESSERE QUINDI TUTTE QUELLE ACCORTEZZE, ANCHE SE NON PRESCRITTE, CHE HANNO COME UNICO SCOPO TUTELARE I DIRITTI E LA RISERVATEZZA DEGLI INTERESSATI

(PER ESEMPIO: *NON RIFERIRE DI FATTI PERSONALI CONOSCIUTI IN VIRTÙ DEL PROPRIO RUOLO PROFESSIONALE, *NON NOMINARE NOMI E COGNOMI ASSOCIATI AD EVENTI PERSONALI IN PRESENZA DI ALTRE PERSONE, *NON CESTINARE DOCUMENTI PERSONALI SENZA AVERLI PRIMA DISTRUTTI, *NON ABBANDONARE DOCUMENTI IN LUOGHI ACCESSIBILI AL PUBBLICO, *NON PRENDERE VISIONE DI DOCUMENTI SE NON NECESSARIO IN BASE ALLA PROPRIA FUNZIONE ECC.)

SCUOLA

REGISTRO DEI TRATTAMENTI (ART. 30)

IL REGISTRO DEI TRATTAMENTI È UN DOCUMENTO CHE SOSTITUISCE L'OBBLIGO DI NOTIFICA ALL'AUTORITÀ DI CONTROLLO DEI TRATTAMENTI DI DATI PERSONALI ED È **OBBLIGATORIO SOPRA I 250 DIPENDENTI e nelle PUBBLICHE AMM.NI** (ANCHE SE LA SUA REDAZIONE È SEMPRE CONSIGLIATA PER IL RISPETTO DEL PRINCIPIO DELL'ACCOUNTABILITY) O IN TUTTI I CASI IN CUI SI EFFETTUANO TRATTAMENTI NON OCCASIONALI DI DATI SANITARI, SINDACALI ECC.

DEVE CONTENERE:

- DATI DEL TITOLARE E DEL RESPONSABILE
- DESCRIZIONE DEI TRATTAMENTI sui DATI
- BASE GIURIDICA DEL TRATTAMENTO
- CATEGORIE DI DATI
- DESTINATARI
- MISURE DI SICUREZZA ADOTTATE
- DURATA DI CONSERVAZIONE DEI DATI
- TRASFERIMENTO O MENO DATI OLTRE CONFINI UE

SCUOLA

Analisi dei rischi e misure di sicurezza

In carico al titolare del trattamento l'obbligo di effettuare l'analisi dei rischi e di vaglio dell'adeguatezza delle misure di tutela.

L'analisi del rischio privacy ha un ruolo fondamentale: diventa lo strumento atto a dimostrare l'adeguatezza delle misure implementate a tutela dei dati trattati.

ART. 32 «Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, si devono mettere in atto misure tali da garantire un livello di sicurezza adeguato al rischio»

I RISCHI DA VALUTARE SONO:

- rischi significativi per i diritti e le libertà fondamentali della persona
- rischio di distruzione accidentale o illegale
- rischio di perdita dei dati
- rischio di modifica non voluta
- rischio di comunicazione e diffusione non consentita

VALUTAZIONE DI IMPATTO (PIA) (ART. 35)

In casi specifici, come il ricorso a tecnologie a rischio per i diritti della persona, trattamenti su larga scala, ecc. (vedi comma 3 Art. 35) il trattamento deve essere testato con una valutazione di impatto privacy, ed eventualmente con una consultazione preventiva al Garante della Privacy

SCUOLA

Estratto dalla lista fornita dal Garante della Privacy
per la protezione dei dati dei rischi che incombono sui sistemi informatici:

- 1. Comportamenti degli operatori:** *Furto di credenziali di autenticazione, *Carenza di consapevolezza, disattenzione o incuria, *Comportamenti sleali o fraudolenti, *Errore materiale
- 2. Eventi relativi agli strumenti:** *Azione di virus informatici o di codici malefici, *Spam o altre tecniche di sabotaggio, *Malfunzionamento, indisponibilità o degrado degli strumenti, *Accessi esterni non autorizzati, *Intercettazione di informazioni in rete
- 3. Eventi relativi al contesto:** *Accessi non autorizzati a locali/reparti ad accesso ristretto, *Asportazione e furto di strumenti contenenti dati, *Eventi distruttivi, naturali o artificiali, dolosi, accidentali o dovuti ad incuria, *Guasto ai sistemi complementari (impianto elettrico, climatizzazione....), *Errori umani nella gestione della sicurezza fisica

SCUOLA

Il sistema sanzionatorio SECONDO IL G.D.P.R. 679/2016

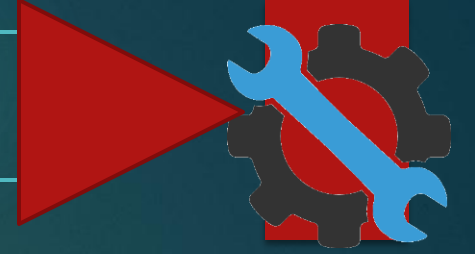
Fino a € 10.000.000,00 O 2% FATTURATO TOTALE ANNUO GLOBALE IN CASO DI VIOLAZIONE DEI SEGUENTI ARTT:

- 8 (consenso dei minori),
- 10 (trattamenti che non richiedono l'identificazione degli interessati),
- 23 (privacy by design e privacy by default),
- 24 (contitolarità del trattamento),
- 25 (nomina rappresentante del Titolare non stabilito nell'Unione Europea),
- 26 (Responsabili del trattamento),
- 27 (istruzioni e autorità del Titolare),
- 28 (documentazione relativa a ciascun trattamento di dati personali),
- 29 (cooperazione con l'autorità di vigilanza),
- 30 (sicurezza del trattamento),
- 31 (notificazione dei data breach all'autorità),
- 32 (comunicazione dei data breach agli interessati),
- 33 (DPIA – Data Protection Impact Assessment),
- 34 (consultazione preventiva dell'autorità di vigilanza),
- 35, 36 e 37 (designazione, posizione e compiti del DPO – Data Protection Officer),
- 39 e 39a (processi di certificazione).

fino a € 20.000.000,00 o fino al 4% del fatturato totale annuo mondiale per le violazioni:

- in materia di principi base del trattamento
- condizioni per il consenso, diritti degli interessati
- trasferimento di dati personali all'estero
- mancata ottemperanza a un ordine o a una limitazione temporanea o definitiva del trattamento disposti dall'autorità di vigilanza.

La SCUOLA in pratica



Le indicazioni del garante

Iscrizioni:

Nell'ambito della scuola pubblica non è necessario acquisire il consenso per trattare i dati personali ai fini dell'iscrizione o di altre attività scolastiche. **Altro discorso problematiche socio-sanitarie**. I dati richiesti non possono riguardare informazioni eccedenti e non rilevanti (es. professione dei genitori o stato di salute dei nonni)

Temi in classe:

Non lede la normativa privacy l'assegnazione di **elaborati** aventi ad oggetto il mondo personale o familiare dell'alunno.

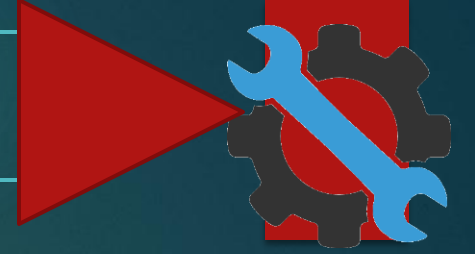
In caso di **lettura in classe** l'insegnante dovrà trovare il giusto equilibrio tra esigenze didattiche e tutela dei dati personali

Restano comunque fermi gli obblighi di segreto professionale o d'ufficio e quelli relativi alla conservazione dei dati personali degli alunni contenuti nei temi.

Voti ed esami:

I voti e gli esiti degli esami sono pubblici. Tuttavia non possono essere pubblicate informazioni sullo **stato di salute** degli alunni (per esempio affetti da dsa). Il riferimento a prove differenziate sostenute da studenti portatori di handicap o con **disturbi specifici di apprendimento** non va inserito nei tabelloni ma solo nell'attestazione da rilasciare allo studente

La SCUOLA in pratica



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 **evitare di inserire**, nelle circolari e nelle comunicazioni scolastiche non rivolte a specifici destinatari, dati personali che rendano identificabili, ad esempio, gli alunni coinvolti in casi di bullismo o in altre vicende particolarmente delicate

Pubblicazioni:

Non si può pubblicare sul sito della scuola, o inserire in bacheca, il nome e cognome degli studenti i cui genitori sono in ritardo nel **pagamento della retta o del servizio mensa**; né può essere diffuso l'elenco degli studenti, appartenenti a famiglie con reddito minimo o a fasce deboli, che usufruiscono gratuitamente di tale servizio.

Gli avvisi messi on line devono avere carattere generale, mentre per comunicazioni di carattere individuale occorre rivolgersi alle singole persone.

Gli istituti scolastici e gli Enti locali non possono pubblicare on line, in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono **dei servizi di scuolabus**, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio.

Tale diffusione di dati personali, che espone i minori a possibili azioni di eventuali malintenzionati, non può assolutamente essere effettuata o giustificata semplicemente affermando che si sta procedendo in tal senso solo per garantire la massima trasparenza del procedimento amministrativo.

La SCUOLA in pratica



Gli istituti scolastici possono pubblicare sui propri SITI INTERNET le **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, devono però contenere solo i dati strettamente necessari all'individuazione del candidato, come il nome, il cognome, il punteggio e la posizione in graduatoria. I dati personali, tra l'altro, non possono rimanere pubblicati on line per un periodo **superiore** a quello previsto.

È invece illecita, perché eccedente le finalità istituzionali perseguite, la pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.

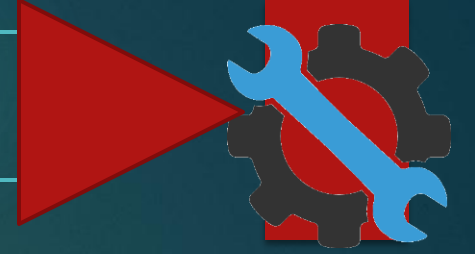
Tale diffusione dei contatti personali incrementa, tra l'altro, il rischio di esporre i lavoratori interessati a forme di **stalking** o a eventuali **furti di identità**.

Disabilità e disturbi specifici dell'apprendimento:

Le istituzioni scolastiche devono prestare particolare attenzione a non diffondere, anche per mero errore materiale, dati idonei a rivelare lo stato di salute degli studenti, così da non incorrere in sanzioni amministrative o penali.

Non è consentito, ad esempio, pubblicare on line una circolare contenente i nomi degli studenti portatori di handicap. Occorre fare attenzione anche a chi ha accesso ai nominativi degli allievi con disturbi specifici dell'apprendimento (DSA), limitandone la conoscenza ai soli soggetti legittimati previsti dalla normativa, ad esempio i professori che devono predisporre il piano didattico personalizzato.

La SCUOLA in pratica



Dalla scuola al lavoro:

Su **esplicita richiesta degli studenti interessati**, le scuole secondarie possono comunicare o diffondere, anche a privati e per via telematica, i dati relativi ai loro risultati scolastici e altri dati personali (esclusi quelli sensibili e giudiziari) utili ad agevolare l'orientamento, la formazione e l'inserimento professionale anche all'estero. Prima di adempiere alla richiesta, gli istituti scolastici devono comunque provvedere a **informare gli studenti su quali dati saranno utilizzati per tali finalità**.

Curriculum e identità digitale dello studente:

La riforma della scuola del 2015 ha istituito il cosiddetto "curriculum dello studente" che, associato a un'identità digitale, raccoglie tutti i dati utili anche ai fini dell'orientamento e dell'accesso al mondo del lavoro, relativi al percorso degli studi, alle competenze acquisite, alle eventuali scelte degli insegnamenti opzionali, alle esperienze formative anche in alternanza scuola-lavoro e alle attività culturali, artistiche, musicali, sportive e di volontariato, svolte in ambito extrascolastico.

Le modalità operative per la sua realizzazione sono demandate a un apposito decreto del Ministro dell'Istruzione, dell'Università e della Ricerca, **sui cui il Garante per la protezione dei dati personali si dovrà esprimere**.

La SCUOLA in pratica



Utilizzo di immagini durante le recite, laboratori didattici e viaggi di istruzione

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 alla eventuale pubblicazione delle medesime immagini su **Internet, e sui social network** in particolare.

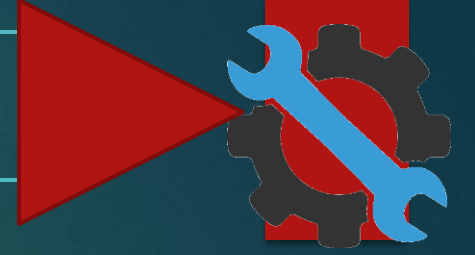
In caso di comunicazione sistematica o diffusione diventa infatti necessario, di regola, ottenere il consenso informato delle persone presenti nelle fotografie e nei video.

Utilizzo dello smartphone

L'utilizzo di telefoni cellulari, di apparecchi per la registrazione di suoni e immagini è in genere consentito, ma esclusivamente per **fini personali**, e sempre nel rispetto dei diritti e delle libertà fondamentali delle persone coinvolte (siano essi studenti o professori) in particolare della loro immagine e dignità.

Le istituzioni scolastiche hanno, comunque, la **possibilità di regolare o di inibire** l'utilizzo di registratori, smartphone, tablet e altri dispositivi elettronici all'interno delle aule o nelle scuole stesse. Gli studenti e gli altri membri della comunità scolastica, in ogni caso, non possono diffondere o comunicare i dati di altre persone (ad esempio pubblicandoli su Internet) senza averle prima informate adeguatamente e averne ottenuto l'esplicito consenso.

La SCUOLA in pratica



LA VIDEOSORVEGLIANZA A SCUOLA

L'INTERESSE DEGLI INDIVIDUI PREVALE SULLA ESIGENZA DI TUTELA DEL PATRIMONIO SCOLASTICO.

QUINDI È possibile installare un sistema di videosorveglianza negli istituti scolastici quando risulti indispensabile per tutelare l'edificio e i beni scolastici, circoscrivendo **PERÓ** le riprese alle sole aree interessate, come ad esempio quelle soggette a furti e atti vandalici.

Le telecamere che inquadrano l'interno degli istituti possono essere attivate solo negli orari di chiusura, quindi non in coincidenza con lo svolgimento di attività scolastiche ed extrascolastiche.

Le aree perimetrali esterne, al pari di ogni altro edificio pubblico o privato, possono invece essere oggetto di ripresa, per finalità di sicurezza, anche durante l'orario di apertura dell'istituto scolastico. In questo caso, l'angolo visuale deve essere delimitato in modo da non inquadrare luoghi non strettamente pertinenti l'edificio.

La presenza di telecamere deve sempre essere segnalata da appositi cartelli (vedi i modelli di informativa semplificata predisposti dal Garante e reperibili sul sito www.garanteprivacy.it), visibili anche di notte qualora il sistema di videosorveglianza sia attivo in tale orario.

Telecamere finte

Installare una videocamera finta a scopo di deterrenza è vietato **IN QUANTO L'ERRATA CONVINZIONE DI ESSERE RIPRESI POTREBBE CONDIZIONARE IMMOTIVAMENTE IL COMPORTAMENTO DELLE PERSONE.**

PRIVACY e COVID



PRIVACY e COVID



Il datore di lavoro può rilevare la temperatura di chiunque all'ingresso della propria sede?

- **DIPENDENTI:** sì, con registrazione del solo superamento della soglia stabilita per legge es. 37,5° (principio di minimizzazione-art.5 par.1 lett.c)
- **ALTRI:**
 - **Maggiorenni:** solo diniego ad entrare
 - **Minorenni:** collocazione in aula COVID e chiamata alla famiglia

PRIVACY e COVID



L'amm.ne può chiedere un' autodichiarazione COVID per l'accesso?

- SI, a TUTTI.
- In ogni caso dovranno essere raccolti solo i dati necessari, adeguati e pertinenti rispetto alla prevenzione del contagio da Covid-19, e astenersi dal richiedere informazioni aggiuntive in merito alla persona risultata positiva, alle specifiche località visitate o altri dettagli relativi alla sfera privata.

PRIVACY e COVID



L'amm.ne può comunicare i Contatti dei funzionari competenti per la prenotazione di servizi in presenza?

- Nel rispetto dei principi di protezione dei dati (art. 5 Regolamento UE 2016/679) la finalità di fornire agli utenti recapiti utili a cui rivolgersi per assistenza o per essere ricevuti presso gli uffici, può essere utilmente perseguita pubblicando i soli recapiti delle unità organizzative competenti (numero di telefono e indirizzo PEC) e non quelli dei singoli funzionari preposti agli uffici. Ciò, anche in conformità agli obblighi di pubblicazione concernenti l'organizzazione delle pubbliche amministrazioni.

PRIVACY e COVID



Quali trattamenti di dati personali sul luogo di lavoro coinvolgono il medico competente?

il medico competente provvede a segnalare al datore di lavoro quei casi specifici in cui reputi che la particolare condizione di fragilità connessa anche allo stato di salute del dipendente ne suggerisca l'impiego in ambiti meno esposti al rischio di infezione. A tal fine, non è invece necessario comunicare al datore di lavoro la specifica patologia eventualmente sofferta dal lavoratore. Cioè, anche nell'emergenza, permane il divieto di informare il datore di lavoro circa le specifiche patologie occorse ai lavoratori.

PRIVACY e COVID



L'amm.ne può segnalare al RLS* i nomi dei dipendenti contagiati?

Di norma NO.

In base al quadro normativo nazionale il datore di lavoro deve comunicare i nominativi del personale contagiato alle autorità sanitarie competenti e collaborare con esse per l'individuazione dei "contatti stretti" al fine di consentire la tempestiva attivazione delle misure di profilassi.

Il RLS comunque nell'espletamento dei propri doveri può venire a conoscenza di casi di contagio.

PRIVACY e COVID



L'amm.ne può rendere noto ai lavoratori l'identità di un collega contagiato?

Di norma NO.

Restano ferme le misure che il datore di lavoro deve adottare in caso di presenza di persona affetta da Covid-19, all'interno dei locali dell'azienda o dell'amministrazione, relative alla pulizia e alla sanificazione dei locali stessi, da effettuarsi secondo le indicazioni impartite dal Ministero della salute

PRIVACY e COVID



L'amm.ne può chiedere ai dipendenti di fare
TEST COVID?

Di norma NO.

Solo il Medico Competente stabilisce la necessità di esami clinici. I datori di lavoro possono offrire ai propri dipendenti, anche sostenendone in tutto o in parte i costi, l'effettuazione di test sierologici presso strutture sanitarie pubbliche e private (es. tramite la stipula o l'integrazione di polizze sanitarie ovvero mediante apposite convenzioni con le stesse), senza peraltro poter conoscere l'esito dell'esame.

PRIVACY e COVID

L'amm.ne può trattare dati di un dipendente affetto da COVID o ne presenta i sintomi?



Di norma NO. Visto però lo stretto legame che intrattiene l'amm.ne con le autorità sanitarie e coi dipendenti che segnalano sintomatologie sospette, il datore di lavoro può trattare i dati relativi ai sintomi o alla positività al Covid-19 del lavoratore per la finalità di salute e sicurezza dei luoghi di lavoro o per adempiere agli obblighi di collaborazione con gli operatori di sanità pubblica. Resta negato il trattamento di dati sulla salute, la comunicazione a terzi e la conoscenza di esiti diagnostici, anche di COVID.

PRIVACY e COVID

Didattica **A** Distanza (DAD)



DPCM 4 marzo 2020 art 1 lett.G
“I dirigenti per il periodo di sospensione delle
attività didattiche adottano la DAD”
è la base giuridica per l’uso della DAD
senza CONSENSO

PRIVACY e COVID



La scuola è tenuta ad acquisire il consenso da alunni, genitori e insegnanti per la DAD?

NO.

Si possono trattare dati ANCHE DATI PARTICOLARI* di insegnanti, alunni(anche minori) e genitori nell'ambito delle proprie finalità istituzionali.

*etnici, politici, religiosi, sindacali, biometrici, sessuali

PRIVACY e COVID



La scuola deve informare gli interessati sui trattamenti dei dati personali nelle attività DAD?

SI.

I tipi di dati, le modalità di trattamento degli stessi, i tempi di conservazione e le operazioni di trattamento, specificando che le finalità perseguite sono limitate esclusivamente all'erogazione della didattica a distanza, sulla base dei medesimi presupposti e con garanzie analoghe a quelli della didattica tradizionale.

PRIVACY e COVID



La scuola può comunicare alle famiglie degli alunni l'identità dei parenti di studenti risultati positivi al COVID 19?

NO.

Spetta alle autorità sanitarie competenti informare i contatti stretti del contagiato, al fine di attivare le previste misure di profilassi. L'istituto scolastico è tenuto a fornire alle istituzioni competenti, le informazioni necessarie, affinché le stesse possano ricostruire la filiera dei contatti del contagiato, nonché, sotto altro profilo, ad attivare le misure di sanificazione recentemente disposte.

PRIVACY e COVID

INFORMATIVA **DAD**



- Misure con cui viene garantito il rispetto del principio di trasparenza nei confronti degli interessati, in particolare attraverso le informazioni che devono essere fornite ai docenti, genitori ed alunni, ai sensi degli artt. GDPR 13 (dati ottenuti presso l'interessato) e 14 (dati NON ottenuti presso l'interessato), con specifico riferimento alle piattaforme scelte.
Nella prossima slide i principali punti da evidenziare.



PRIVACY e COVID

INFORMATIVA **DAD**



1. Titolare
2. Responsabile/i
3. Base giuridica
4. Finalità
5. Tipi di dati
6. Destinatari
7. Trasferimento fuori GDPR
8. Conservazione: art.5 c.1 lett.e (es. durata account piattaf.)
9. Diritti dell'interessato
10. Profilazione (art.22 parr.1 e 4)
11. Uso dei dati in altri trattamenti
12. Eventuale valutazione di impatto (art 35)

PRIVACY e COVID



INFORMATIVA **DAD**

- Misure tecniche ed organizzative adottate al fine di garantire un'adeguata sicurezza dei dati personali trattati tramite la Piattaforma DAD (regolamento di comportamento e sicurezza informatica)

Es: registrazione lezioni, inquadratura oggetti e affissioni, inquadrature di terzi, uso **Virtual Private Networks**, Ip/MAC address, O.S., Geolocalizzazione

PRIVACY e COVID

Caratteristiche PIATTAFORMA DAD



- Strumento qualificato AgID
- **Uso dati NON a scopo pubblicitario**
- Solo fini previsti dal PTOF (sarà utile inserire un progetto di didattica nel PTOF relativo alla piattaforma usata per evitare eventuali consensi ulteriori)
- **Comportamento alunni NON PROFILATO**
- Regolamento sugli strumenti scelti

PRIVACY e COVID

PIATTAFORME DAD (da sito MIUR)



- G Suite for education (hangout)
- Office 365 Education (Teams)
- WESCHOOL TIM



G Suite For Education



Office 365



WESCHOOL



PRIVACY e COVID

ESEMPIO DI PIATTAFORMA COMPLIANT



Nel caso di piattaforma GOOGLE G-Suite for education, esiste un contratto con Google Ireland Limited che, anche se gratuito, contrattualizza la figura di RESPONSABILE ESTERNO

PRIVACY e COVID



ESEMPIO DI PIATTAFORMA COMPLIANT

piattaforma G SUITE for education:

Rispetto del regolamento

<https://cloud.google.com/security/gdpr?hl=it>

Presenza nel catalogo dei servizi AgID qualificati

<https://cloud.italia.it/marketplace/service/690>

Conformità e certificazioni

<https://cloud.google.com/security/compliance/privacy-shield>

Contratto (con dichiarazione di Responsabile per GOOGLE)

https://gsuite.google.it/intl/it/terms/education_terms.html

Informativa sulla privacy di G Suite

https://gsuite.google.it/intl/it/terms/education_privacy.html

PRIVACY e COVID

Non è tutto **oro** quello che riluce...



- ✓ Gmail
- ✓ Calendar
- ✓ Classroom
- ✓ Jamboard
- ✓ Contatti
- ✓ Drive
- ✓ Documenti



*Solo questi sono compliant con GDPR per la Scuola!

- ✓ Moduli
- ✓ Gruppi
- ✓ Fogli
- ✓ Sites
- ✓ Presentazioni
- ✓ Talk/Meet
- ✓ Vault

PRIVACY e COVID

Non è tutto **oro** quello che riluce...

Non è detto che p.es. YouTube™ non possa essere usato nella scuola, ma per poter essere *compliant* dovrà venire configurato come servizio “passivo”, ovvero solo in lettura. Questo impedirà agli studenti di pubblicare su YouTube™.

Analoghe considerazioni sugli altri servizi aggiuntivi (non principali).



PRIVACY e COVID

Servizi	Servizi principali di G Suite for Education	Servizi aggiuntivi
Termini	Informativa sulla privacy di G Suite for Education	
	<u>Contratto di G Suite for Education ed Emendamento sull'elaborazione dei dati</u> (se accettato dalla scuola)	<u>Termini di servizio</u> e <u>Norme sulla privacy</u> di Google, nonché <u>termini di servizio specifici</u>
Utilizzo dei dati	Le informazioni personali degli utenti raccolte nei servizi principali vengono utilizzate al solo scopo di fornire all'utente i servizi principali come Gmail, Documenti, Fogli e Presentazioni.	Le informazioni contenute in tutti i servizi aggiuntivi possono essere utilizzate per fornire, mantenere, proteggere e migliorare tali servizi e per svilupparne di nuovi.
Annunci	Non sono presenti annunci nei servizi principali. Nei servizi principali come in quelli aggiuntivi, i dati dei clienti non vengono mai utilizzati a scopi di pubblicità.	I servizi aggiuntivi possono contenere annunci pubblicitari. Per gli utenti di G Suite for Education delle scuole primarie e secondarie, Google non utilizza alcuna informazione personale (o associata a un Account Google) per definire il target degli annunci.
Sicurezza	I servizi principali sono inclusi nei controlli di sicurezza e nelle certificazioni di G Suite (ISO 27001, SOC 2 e SOC 3).	Tutti i servizi aggiuntivi rispettano gli elevati standard di Google nel campo della <u>sicurezza delle informazioni</u> .
Limiti di condivisione	Google non condivide con terze parti i dati dei clienti che sono contenuti nei servizi principali, tranne nei pochi casi <u>specificati nella nostra Informativa sulla privacy</u> (ovvero dietro consenso del cliente o nei casi previsti dalla legge). Le disposizioni contrattuali in materia di riservatezza di G Suite limitano inoltre i modi in cui i dati dei clienti contenuti nei servizi principali possono essere condivisi con terze parti.	Google non condivide le informazioni personali con terze parti, tranne nei pochi casi <u>specificati dalla nostra Informativa sulla privacy</u> (ovvero dietro consenso del cliente o nei casi previsti dalla legge).

PRIVACY e COVID



NUOVO Utente in Piattaforma DAD

- Consenso NON NECESSARIO
- nome.cognome@nomescuola.it
- Password= “cambiami”
- Necessario cambiare password al primo accesso → consenso implicito

SCUOLA



GRAZIE !