“La protezione dei dati personali nelle Istituzioni scolastiche”

a cura dell’avv. Valerio De Feo

Obiettivi del corso

- Analizzare le questioni aperte correlate all'uso dei dati personali da parte di tutti coloro che ruotano attorno alla comunità scolastica, tenendo presente che abbiamo dei neo DS in servizio da poco tempo

- Fornire indicazioni utili per affrontare casi concreti e soprattutto per prevenire casi di contenzioso per il Dirigente e il suo staff

- In generale, affrontare i temi del corso con taglio estremamente pratico, fornendo strumenti critici pronti per un uso immediato e coinvolgendo i corsisti nell'analisi dei casi.

Capitolo 1
Le fonti

Le fonti normative

Il Regolamento UE 2016/679 del 27 aprile 2016 concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati.

Il D.Lgs n.101 del 10 agosto 2018 modifica il «vecchio» Codice Privacy italiano (D.Lgs 196/2003) per adeguarlo al Regolamento.

Il vecchio codice viene riformato in modo sostanziale, proprio in ragione della preminenza del Regolamento Europeo.

Poi c’è il ruolo determinante del «Garante Privacy»

Interventi sotto il controllo del Garante della Privacy

- Misure di garanzia, con particolare riguardo ai dati sulla salute
- Verifica Autorizzazioni Generali
- Decisioni su casi contenzioso
- Regole deontologiche (ad es. per i trattamenti nell’ambito dei rapporti di *lavoro)*
- *Precisazioni sulle attività sottoposte a valutazione d’impatto*

«……intanto restano operative i precedenti provvedimenti a carattere generale, come ad esempio, quelli sulla videosorveglianza e sull’amministratore di sistema, in quanto compatibili con il GDPR»

Cominciamo a ragionare su…

Peculiarità del contenzioso in materia di protezione dei dati personali

- I casi di contenzioso come possono evolvere e dove possono approdare?
- Attenzione sulle risposte da dare a genitori e dipendenti
- Attenzione a cosa si pubblica sul sito della scuola
- Attenzione a come si usa il registro elettronico
- Attenzione alla formazione del personale
- Perché il Garante si attiva sulle scuole molto più di quello che si pensi…
- Differenze e integrazione con i casi di contenzioso in materia civile, penale, di responsabilità per danno erariale, amministrativo

Capitolo 2
Principi da cui partire….

Quadro generale di riferimento…

- **È importante entrare nella logica della responsabilizzazione (*accountability*)**

- **Il Garante nei convegni: «poter dimostrare policy e processi conosciuti dall'organizzazione in relazione ai rischi per i diritti degli interessati»**

- **"privacy by design", garantire la protezione dei dati sin dalla fase di ideazione e progettazione di un trattamento (anche nella scelta dei fornitori) o di un sistema di trattamenti**

- **principio della minimizzazione del rischio, privacy by default (dati anonimi preferibilmente, poi dati «comuni» e poi, proprio se è indispensabile, i dati di cui agli artt. 9 e 10 del Regolamento che una volta chiamavamo sensibili e giudiziari)**

Dopo la nomina del DPO, abbiamo più o meno individuato 6 aree di lavoro

1) Rendere l'informativa, NO CONSENSO (informative idonee per minori);

2) Individuazione Banche Dati e Analisi dei rischi/Valutazione d'impatto

3) Individuazione e messa in opera delle misure di sicurezza

4) Nominare Responsabile del trattamento esterno e gli Autorizzati al trattamento (ex incaricati, il Codice «rilancia» anche la formazione)

5) Tenere il registro dei trattamenti (Schema registro Nota MIUR n. 877 del 03/08/2018)

6) Tenere il registro delle violazioni

Riepiloghiamo quindi i soggetti coinvolti nel trattamento dei dati

TITOLARE: 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

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

INCARICATO/AUTORIZZATO: Persone fisiche autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile

INTERESSATO: Persona fisica resa identificabile dai dati personali trattati. NB: Interessato non è mai una persona giuridica.

DPO: Responsabile della protezione dei dati in azienda/ente.
Sorveglia e informa il titolare riguardo agli obblighi derivanti dalla normativa

Capitolo 3
Alcune indicazioni/memo partendo anche dal Codice italiano….

Osservazioni/memo 1

1) Lavoriamo solo sui dati delle persone fisiche, in qualsiasi modo trattati
2) La base giuridica di partenza del trattamento delle scuole sta nell'articolo 6 del GDPR (trattamenti per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri)
3) Tradotto nell'ordinamento giuridico italiano, serve una norma di legge o, nei casi previsti dalla legge, di regolamento (intendendo in questo caso un DPR, un DM, un DPCM, ecc)

Osservazioni/memo 2

1) **Comunicazioni tra titolari di dati diversi da quelli di cui agli artt 9 e 10 del Regolamento (ad esempio, comunicazioni tra due scuole), per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri: solo se prevista da norme di Legge o di Regolamento, oppure se decorso termine di 45 gg dalla relativa comunicazione al Garante, senza diversa determinazione del Garante medesimo**
2) **La Diffusione e la comunicazione a soggetti non pubblici: solo se prevista da norma di legge**

Osservazioni/memo 3

1) **I vecchi dati sensibili (salute, convinzioni politiche, religiose e filosofiche, appartenenza sindacale, origine razziale o etnica dati genetici, biometrici, vita e orientamento sessuale delle persone) ora sono previsti dall'art. 9 del Regolamento Europeo e si trattano per motivi di interesse pubblico in modo proporzionato alla finalità perseguita**
2) **Il codice italiano individua i motivi di interesse pubblico: accesso, istruzione e formazione…., instaurazione e gestione rapporti di lavoro, materie sindacali, previdenziali, fiscali, sicurezza sul lavoro, responsabilità civile, disciplinare, contabile, attività ispettiva**
3) **Poi servono anche disposizioni di Legge e Regolamento (DM 305 2006?)**

Osservazioni/memo 4

1) **Tra i dati di cui all'art. 9 del GDPR (come detto ex dati sensibili) i dati sulla salute, quelli genetici e i biometrici prevedono richiedono una garanzia ulteriore→**

2) **Misure di garanzia del Garante (cifratura, pseudonimizzazione, minimizzazione, accesso selettivo ai dati) e resta il divieto di diffusione**

Osservazioni/memo 5

1) I vecchi dati giudiziari (condanne penali, reati misure di sicurezza) ora sono previsti dall'art. 10 del Regolamento Europeo e si trattano solo se il trattamento è previsto da norma di legge o di regolamento in determinate materie, vediamo quelle di interesse delle scuole

2) Rapporti di lavoro, diritto di accesso, comunicazioni antimafia, documentazione per partecipare a appalti, requisito idoneità morale, difesa dei diritti in sede giudiziari

3) Servono quindi anche qui disposizioni di Legge e Regolamento (DM 305 2006?)

Osservazioni/memo 6

1) **Resta il vecchio articolo 96 del Codice leggermente riformato (comunicazione o diffusione, su richiesta degli interessati, degli esiti formativi intermedi e finali, sempre previa informativa)**

«Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale, anche all'estero, le istituzioni del sistema nazionale di istruzione, i centri di formazione professionale regionale, le scuole private non paritarie nonché le istituzioni di alta formazione artistica e coreutica e le università statali o non statali legalmente riconosciute **su richiesta degli interessati**, **possono comunicare o diffondere, anche a privati e per via telematica**, dati relativi agli esiti formativi, intermedi e finali, degli studenti e altri dati personali **diversi da quelli di cui agli *articoli 9* e *10* del *Regolamento***, pertinenti in relazione alle predette finalità e indicati nelle informazioni rese agli interessati ai sensi dell'*articolo 13 del Regolamento*. I dati possono essere successivamente trattati esclusivamente per le predette finalità».

Viene aggiunto (ma non serviva) che restano ferme le vigenti disposizioni in materia di pubblicazioni dell'esito degli esami mediante affissione nell'albo dell'Istituto e di rilascio di diplomi e certificati

Osservazioni/memo 7

1) **Resta per ora immutata, di fatto, la materia della videosorveglianza e il rapporto tra privacy e accesso, inteso nelle sue varie accezioni**

2) **Resta fuori la materia dei minori che hanno compiuto 14 anni e possono esprimere il consenso al trattamento in relazione ai servizi della società dell'informazione**

Osservazioni/memo 8

1) **Resta il limite ai diritti dell'interessato, ove dall'esercizio dei diritti possa derivare un pregiudizio alla riservatezza dell'identità del dipendente che segnala ai sensi della Legge 30 novembre 2017, n. 179 l'illecito di cui sia venuto a conoscenza in ragione del proprio ufficio**

2) **Ricezione curricula spontanei, informativa al primo contatto utile, il consenso, nei limiti di cui all'art. 6, paragrafo 1, lettera b) del GDPR, NON è dovuto**

3) **FOTO e VIDEO Resta, sostanzialmente, il debolissimo appiglio della norma di cui all'articolo 136, comma 1 lettera c del Codice (pubblicazione e diffusione anche occasionale, di articoli…altre manifestazioni del pensiero), nel rispetto di regole deontologiche**

Capitolo 4
Le misure di sicurezza
Nota MIUR n. 877 del 03/08/2018

Misure specifiche per la protezione dei dati

ID	MISURA	DESCRIZIONE
MPD-1	**Minimizzazione della quantità di dati personali**	Misure volte a gestire solo dati personali adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati.
MPD-2	**Partizionamento dei dati**	Misure volte a separare le aree di archiviazione dei dati personali trattati al fine di ridurre la possibilità che i dati possano essere correlati e compromessi, ad esempio attraverso la creazione di cartelle di rete condivise distinte per tipologia di dati personali o l'archiviazione di documentazione cartacea in faldoni o archivi separati.
MPD-3	**Cifratura**	Misure volte ad assicurare la riservatezza dei dati personali archiviati (in database, documenti e archivi elettronici, etc.) o trasmessi attraverso le reti (ad es., VPN, HTTPS, TLS, etc.) e per gestire chiavi crittografiche

Misure specifiche per la protezione dei dati

ID	MISURA	DESCRIZIONE
MPD-4	**Pseudonimizzazione**	Misura tecnica volta a rendere anonimi e non riconducibili alla persona i dati personali trattati attraverso sistemi informatici, ad esempio attraverso l'uso di identificativi numerici in sostituzione del nome e cognome della persona.
MPD-5	**Controllo degli accessi logici ed autenticazione**	Misure volte ad attuare e implementare la politica di controllo degli accessi logici ai dati personali trattati attraverso sistemi informatici (ad es., politiche di accesso ad applicativi o a cartelle di rete condivise), secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti. Tale politica si basa sul principio della minima conoscenza: ogni utente ha accesso ai soli dati personali strettamente necessari per lo svolgimento dei propri compiti.
MPD-6	**Cancellazione sicura**	Misura adottata allo scopo di eliminare e distruggere irreversibilmente i dati personali, ad esempio attraverso la smagnetizzazione di un supporto informatico o la distruzione di documenti cartacei, in modo che non possano essere recuperati dal supporto su cui sono archiviati.

Misure generali di sicurezza fisica e logica

ID	MISURA	DESCRIZIONE
MGS-1	**Sicurezza dell'ambiente operativo**	Misure adottate per gestire la configurazione di sicurezza di server e database che costituiscono la spina dorsale del sistema di elaborazione dei dati personali, applicando politiche specifiche in funzione della rilevanza dei dati personali trattati dall'applicazione ospitata. Tali misure si applicano anche alla protezione delle applicazioni, in particolare di quelle Web.
MGS-2	**Sicurezza della rete e delle comunicazioni**	Misure adottate per proteggere i dati personali durante il transito attraverso la rete, sia per le connessioni esterne (Internet), sia per l'interconnessione con i sistemi del MIUR. A seconda della tipologia di canale sul quale il trattamento è effettuato, gli strumenti di protezione adottati comprendono: firewall, sonde di rilevamento intrusione e altri dispositivi attivi o passivi di sicurezza della rete, protocolli di cifratura, politiche di controllo dei cookies, etc.

Misure generali di sicurezza fisica e logica

ID	MISURA	DESCRIZIONE
MGS-3	**Tracciatura e monitoraggio**	Misure per la registrazione delle attività eseguite su sistemi informatici dagli utenti e dagli amministratori di sistema su dati personali e sistemi di sicurezza, al fine di consentire il tracciamento delle operazione svolte. Il monitoraggio delle registrazioni prodotte (c.d. “file di log”), inoltre, consente l’identificazione di potenziali tentativi interni o esterni di violazione del sistema e la rilevazione tempestiva di incidenti relativi a dati personali (ad es., eventi di diffusione, modifica o distruzione non autorizzate di dati personali), fornendo al tempo stesso gli elementi di prova nel contesto delle indagini.
MGS-4	**Gestione sicura del cambiamento**	Esistenza ed attuazione di un processo operativo di gestione sicura del cambiamento al fine di controllare, attraverso verifiche e approvazioni, le modifiche eseguite nel sistema IT utilizzato per il trattamento dei dati personali. Ogni modifica deve essere registrata e la data/orario dell’ultima modifica deve essere conservata.

Misure generali di sicurezza fisica e logica

ID	MISURA	DESCRIZIONE
MGS-5	**Gestione sicura dell'hardware, delle risorse e dei dispositivi**	Misure adottate per gestire l'inventario e la configurazione di sicurezza dell'hardware, delle risorse di rete e dei dispositivi (server, periferiche, dispositivi di comunicazione, etc.) utilizzati per il trattamento dei dati personali.
MGS-6	**Gestione sicura delle postazioni di lavoro**	Misure adottate per gestire la configurazione di sicurezza delle postazioni di lavoro degli utenti fisse e portatili (ad es., impostazioni del sistema operativo, applicazioni, software di office automation, etc.). Tali politiche impediscono agli utenti di eseguire azioni che potrebbero compromettere la sicurezza del sistema IT (ad es., la disattivazione di programmi antivirus o l'installazione e l'esecuzione di software non autorizzato, accesso a siti potenzialmente pericolosi)

Misure generali di sicurezza fisica e logica

ID	MISURA	DESCRIZIONE
MGS-7	**Backup e Continuità operativa**	Esistenza ed attuazione di politiche che stabiliscono le modalità di salvataggio dei dati personali, allo scopo di assicurarne la disponibilità e l'integrità nel tempo, e di ripristino dell'operatività a seguito di un evento avverso, ossia le procedure operative e le misure tecniche da seguire per ripristinare la disponibilità e l'accesso ai servizi essenziali in caso di incidente che ne pregiudichi l'operatività.
MGS-8	**Manutenzione delle apparecchiature**	Esistenza e attuazione di politiche per la manutenzione periodica delle apparecchiature di continuità elettrica, dei sistemi antincendio e di ogni altra tipologia di sistema a supporto dell'operatività dei sistemi informativi.
MGS-9	**Protezione dalle fonti di rischio ambientali**	Misure adottate per ridurre o contenere i rischi connessi a minacce ambientali (fenomeni climatici, incendi, allagamenti) che potrebbero influire sull'operatività dei sistemi informativi, sulla continuità dei servizi erogati e sulla sicurezza dei dati personali trattati. Esempi sono: gruppi di continuità, sistemi antincendio, armadi ignifughi, etc.

Misure organizzative e processi di governo

ID	MISURA	DESCRIZIONE
MOG-1	**Modello Organizzativo e di Gestione**	Il modello organizzativo e di gestione della privacy costituisce il fondamento per la sicurezza dei dati personali trattati dall'organizzazione, definendo i processi volti a controllare i rischi che i trattamenti dell'organizzazione pongono sui diritti e le libertà delle persone interessate e individuando ruoli e responsabilità di chi ha accesso ai dati personali, in base al principio del minimo privilegio. Un ruolo di particolare importanza è svolto dal Responsabile della Protezione dei Dati (RPD), che monitora la conformità al regolamento e collabora con il Titolare nell'adeguare le misure di protezione dei dati personali trattati.
MOG-2	**Politiche e procedure per la protezione dei dati personali**	La politica per la protezione dei dati personali dimostra l'impegno generale alla protezione dei dati personali e definisce i principi di base per la loro sicurezza e protezione. Il documento formalizza gli obiettivi e le regole da applicare nel campo della protezione dei dati e costituisce la base per l'attuazione delle misure tecniche e organizzative specifiche richieste dall'art. 32 del RGPD. Le specifiche misure tecniche e organizzative attuate sono descritte in procedure operative di dettaglio che indirizzano temi specifici (ad esempio controllo degli accessi, gestione dei dispositivi, gestione delle risorse, ecc.).

Misure organizzative e processi di governo

ID	MISURA	DESCRIZIONE
MOG-3	**Gestione dei Responsabili del trattamento e delle terze parti**	I rapporti con fornitori esterni di servizi che hanno accesso a o trattano dati personali per conto del Titolare devono essere formalizzati tramite un contratto o altro atto legale stabilito e siglato tra le parti, in cui è disciplinato il trattamento da parte del responsabile e specificate le misure tecniche e organizzative adottate nel rispetto dei requisiti del RGPD e a garanzia della tutela dei diritti dell'interessato
MOG-4	**Sicurezza del ciclo di vita delle applicazioni e nei progetti**	Misure specifiche predisposte per garantire che si considerino i requisiti di protezione dei dati personali e l'applicazione delle più severe impostazioni sulla privacy sin dalle prime fasi del processo di sviluppo di un sistema informativo e durante il ciclo di vita delle applicazioni, nel rispetto dei principi di "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita" introdotti dall'art. 25 del RGPD.

Misure organizzative e processi di governo

ID	MISURA	DESCRIZIONE
MOG-5	**Gestione degli Incidenti di sicurezza e delle Violazioni dei dati personali**	Nel caso si verifichino incidenti di sicurezza che comportano la "distruzione, perdita, modifica, divulgazione non autorizzata o accesso ai dati personali trasmessi, conservati o comunque trattati" (cfr. art. 4.12 del RGPD), sono attivate procedure per la gestione di tali eventi e la notifica all'autorità di controllo e alle persone interessate.
MOG-6	**Gestione e formazione del personale**	Misure specifiche predisposte per garantire che il personale coinvolto nel trattamento dei dati personali sia adeguatamente informato in merito agli obblighi di riservatezza, specialmente per il personale chiave coinvolto nel trattamento dei dati personali ad alto rischio, e sensibilizzato sulle procedure di sicurezza e protezione dei dati (ad esempio uso di password e accesso a specifici sistemi di elaborazione e trasmissione dati).

Misure organizzative e processi di governo

ID	MISURA	DESCRIZIONE
MOG-7	**Controllo degli accessi fisici**	Misure volte ad assicurare la sicurezza fisica e il controllo degli accessi agli edifici e alle zone in cui sono ospitate le risorse a supporto del trattamento (documenti cartacei e strumenti informatici), ad esempio attraverso un servizio di portineria, l'uso di tornelli con autenticazione tramite badge di riconoscimento e porte chiuse a chiave.
MOG-6	**Sicurezza dei documenti cartacei**	Politiche e processi di gestione dell'archivio per assicurare che i documenti cartacei contenenti dati personali utilizzati durante il trattamento siano prodotti, archiviati, consultati, trasmessi e distrutti nel rispetto dei diritti dell'interessato.

Capitolo 5 – Emergenza sanitaria e dintorni

Iniziamo dalla «Sentenza Schrems II»….

1) La Corte di giustizia dell'Unione Europea (CGUE) ha, il 16 Luglio 2020, pronunciato la c.d «Sentenza Schrems II» in materia di trasferimento di dati personali tra l'Unione Europea e gli Stati Uniti

2) L'approdo finale della Corte è che la normativa americana, oggetto di valutazione, non fornisce un livello adeguato di protezione in materia di trattamento dei dati personali, tale da essere sostanzialmente equivalente a quello dell'UE.

3) Il risultato è che le vecchie clausole standard non sono sufficienti e dovrebbero essere contrattate misure supplementari con il fornitore, lavoro alquanto complesso e macchinoso per le scuole….

Quali scelte e azioni possibili…

Evidentemente tutto parte da una valutazione con il DPO sulle piattaforme che vengono utilizzate… La scelta diventa, dunque, tra tre opzioni:

1) **utilizzare piattaforme che mantengono dati in Italia o in Europa;**

2) **se si resta con un fornitore che conserva dati negli USA, concordare con il DPO politiche di riduzione del rischio (meno dati personali possibili nei testi mail, nei documenti allegati, meno documenti possibili nei repository fuori UE, per le video conferenze nomi incompleti e sistemi con cifratura end to end, dati il più possibile anonimi quando si usano sistemi di messaggistica, ecc, ecc)**

3) **(ipotesi nettamente più complicata) contrattare misure supplementari con il fornitore USA…….**

Con le linee guida sulla DDI il 7 agosto 2020 interviene il MIUR

1) **Le linee guida si aggiungono alla Nota dipartimentale MIUR 17 marzo 2020, n. 388 seguita dal Provvedimento Garante Privacy del 26 marzo 2020, n. 64. Il MIUR ribadisce alcuni concetti essenziali**

2) **Raccogliere solo dati personali strettamente pertinenti e per un tempo limitato; uso di piattaforme che rispondano ai necessari requisiti di sicurezza dei dati a garanzia della privacy; tenere conto delle opportunità di gestione già presenti all'interno del registro elettronico; possibile oscuramento dell'ambiente circostante in didattica sincrona; rilevazione presenze con registro elettronico; comunicazioni scuola-famiglia e annotazione dei compiti con registro elettronico; formare i dipendenti sull'uso di repository in locale o in cloud; definire politiche di conservazione dei documenti ufficiali della scuola; integrare il Regolamento d'Istituto con disposizioni sul comportamento da tenere durante i collegamenti; indicazioni ai docenti sul setting "d'aula" virtuale**

Su DDI e tutela della privacy interviene poi il MIUR il 4 settembre 2020 in accordo con il Garante privacy

1) **Di seguito i principi e i concetti fondamentali evidenziati**

2) **Trattamento solo per scopi istituzionali; scelta dei fornitori con il DPO; consenso non richiesto; informativa completa anche sulle piattaforme; cancellazione dati al termine del progetto didattico; nomina del fornitore come resp. del trattamento con dati trattati solo per finalità didattiche; minimizzazione dei trattamenti; se dati sono trasferiti fuori UE, occorre verificare che sussistano tutti i presupposti giuridici richiesti dalla disciplina per assicurare un adeguato livello di protezione; accessi autorizzati alle piattaforme solo per la propria parte di lavoro; regolamentare uso webcam; usare "disclaimer" per ammonire rispetto ai rischi che la diffusione delle immagini e, più in generale, delle lezioni può comportare, nonché le responsabilità di natura civile e penale; materiale caricato in piattaforma solo se inerente all'attività didattica; no valutazione di impatto generalizzata; definizione misure di sicurezza**

Capitolo 6 - Altre indicazioni di interesse delle scuole

Annotazioni sul registro elettronico di dati particolari

Garante per la protezione dei dati personali - Delibera 05/03/2020 n. 45

E' vietata la pubblicazione nella sezione del registro elettronico consultabile attraverso credenziali di accesso da parte delle famiglie di tutti gli studenti di una classe di una nota riguardante informazioni relative alla salute di uno studente

Il caso riguardava una nota con informazioni relative alle visite mediche periodiche a cui doveva sottoporsi uno studente

«Tali informazioni, alla luce del principio di minimizzazione, avrebbero dovuto essere rese visibili esclusivamente alla famiglia dell'alunno interessato ed eventualmente agli altri docenti della classe impegnati nelle lezioni del mercoledì, per le sopra richiamate esigenze didattiche e di valutazione, mentre, sotto altro profilo, va considerato che non esiste alcuna disposizione che preveda la messa a disposizione, tramite il registro elettronico, dei dati oggetto del reclamo a tutte le famiglie degli alunni frequentanti la classe»

Errori nelle comunicazioni via mail…

Garante per la protezione dei dati personali - Ordinanza 09/01/2020 n. 1

Dichiarato illecito il trattamento effettuato dalla Provincia autonoma di Trento, consistente nell'invio di una e-mail con allegata la nota del Dipartimento XX (prot. n. XX) a sedici indirizzi di posta elettronica, in chiaro, afferenti alle famiglie dei minori non in regola con l'assolvimento degli obblighi vaccinali.

Affissione dati non consentita all'ingresso della scuola

Garante per la protezione dei dati personali - Ordinanza 02/07/2020 n. 117

Integra un illecito trattamento dei dati personali la diffusione, mediante affissione sulla porta di ingresso della scuola, di elenchi contenenti dati personali di soggetti minorenni (nomi degli alunni, date di nascita, indirizzi di residenza, numeri di telefono o annotazioni del tipo «manca copia vaccino).

Il trattamento di dati personali effettuato in ambito pubblico è lecito solo se strettamente necessario per adempiere un obbligo legale al quale è soggetto il titolare del trattamento oppure per l'esecuzione di un compito di interesse pubblico e deve avvenire nel rispetto dei principi di liceità, nonché di minimizzazione dei dati.

Pubblicazione dati alunni sul sito web non consentita

Garante per la protezione dei dati personali - Ordinanza 09/07/2020 n. 140

E' vietata la pubblicazione di informazioni personali degli alunni tra cui "dati relativi alla dispersione, alle insufficienze, all'isee, alla disabilità ecc." afferenti ad una graduatoria per la partecipazione ad un progetto didattico.

Nel caso in esame, la segreteria della scuola aveva erroneamente pubblicato sul sito web e all'albo pretorio le graduatorie provvisorie e definitive riferite al reclutamento degli alunni partecipanti ad un progetto didattico elaborate in fase procedurale, da tenersi esclusivamente agli atti d'ufficio perché contenenti dei dati sensibili riferiti agli alunni partecipanti e relativi alla situazione economica, all'insufficiente situazione didattico-educativa ed alla disabilità, anziché pubblicare le graduatorie contenenti solo il punteggio finale assegnato ad ogni alunno

Pubblicazione non pertinente dati graduatorie

Garante per la protezione dei dati personali - Ordinanza 30/01/2020 n. 21

La pubblicazione sul sito della scuola, nell'ambito delle graduatorie di istituto, di dati non necessari rispetto alle finalità perseguite con la pubblicazione della graduatoria integra una fattispecie di illecito trattamento dei dati personali.

Si trattava nel caso di dati quali codice fiscale, indirizzo, numero di telefono fisso e mobile, indirizzo email, ecc.

Pubblicità esiti intermedi e finali - 1

Ministero dell'Istruzione - Nota 09/06/2020 n. 9168

Pubblicazione on line degli esiti degli scrutini delle classi intermedie va intesa come in via esclusiva nel registro elettronico.

«Ammesso" e "non ammesso" sono pubblicati, distintamente per ogni classe, nell'area riservata del registro elettronico a cui accedono tutti gli studenti della classe di riferimento.

I voti sono riportati, oltre che nel documento di valutazione, anche nell'area riservata del registro elettronico a cui può accedere il singolo studente mediante le proprie credenziali personali.

"Disclaimer" con cui si informino i soggetti abilitati all'accesso che i dati personali ivi consultabili non possono essere oggetto di comunicazione o diffusione (ad esempio mediante la loro pubblicazione anche su blog o su social network).

Pubblicità esiti intermedi e finali - 2

Ministero dell'Istruzione - Nota 09/06/2020 n. 9168

Se la scuola non ha il registro, pubblicazione all'albo della scuola (?!) con la sola indicazione di ammissione/non ammissione (per non più di 15 giorni)

Stessi principi per esiti degli scrutini di ammissione agli esami di Stato conclusivi del secondo ciclo di istruzione:

"Ammesso" e "non ammesso" pubblicati, distintamente per ogni classe, nell'area in cui accedono tutti gli studenti della classe di riferimento.

I voti in decimi riferiti alle singole discipline sono riportati, oltre che nel documento di valutazione, nell'area riservata del registro

Pillole di giurisprudenza

Corte di Cassazione - Sezione Seconda - Ordinanza 03/09/2020 n. 18292
Albo on line: illegittima la pubblicazione dei dati per un periodo superiore a 15 giorni (è ammesso un termine maggiore, ma non deve trattarsi di dati particolari e devono esserci prescrizioni normative o evidenti necessità della PA stessa)

T.A.R. LOMBARDIA - MILANO - Sezione Terza - Sentenza 28/09/2020 n. 1721
Sussiste il diritto di accesso agli atti del procedimento disciplinare da parte dell'autore dell'esposto che abbia dato luogo a un procedimento disciplinare

T.A.R. LOMBARDIA - MILANO - Sezione Terza - Sentenza 25/05/2020 n. 920
Classificare atti come "riservati" non basta a sottrarli al diritto di accesso; questa classificazione è di per sé inidonea a disvelare la presenza di dati personali sensibili riferiti a terzi (si trattava di procedimento disciplinare).

Tracce di lavoro per i laboratori

Corte dei Conti LAZIO - Sentenza 28/05/2019 n° 246

- **Leggere il testo**
- **Evidenziare le principali questioni rilevanti in relazione alla gestione della scuola**
- **Prospettare i principali errori commessi in un'ottica costruttiva e di miglioramento**

Delibera Garante Privacy 29/07/2020 n° 149

- **Leggere il testo**
- **Evidenziare le principali questioni rilevanti in relazione alla gestione della scuola**
- **Prospettare i principali errori commessi in un'ottica costruttiva e di miglioramento**

“Grazie a tutti!!!”

Avv. Valerio De Feo

info@italiascuola.it