PRIVACY

NORMATIVA. D. Lgs. 30 giugno 2003, n. 196 (Codice della privacy). L. 27 dicembre 2019, n. 160. D.L. 14 giugno 2019, n. 53. D.M. 15 marzo 2019. D. Lgs. 10 agosto 2018, n. 101 (Decreto di adeguamento al GDPR). Decreto Ministeriale 7 dicembre 2006. Linee guida Garante Privacy lavoro pubblico 2007. L. 15/2009. Videosorveglianza 2004 e 2010. Videotelefonini: Dir. 15.03.2007 Dir. 20.11.2007. Garante per la protezione dei dati personali «Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati» (Allegato alla deliberazione n. 243 del 15 maggio 2014). D. lgs. 14 marzo 2013 n. 33 intitolato «Riordino della disciplina riguardante gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni». Circolare MIUR 563 del 22 maggio 2018, che raccomanda alle Istituzioni Scolastiche la nomina del D.P.O.

REGOLAMENTO GENERALE PER LA PROTEZIONE DEI DATI PERSONALI. Il Regolamento generale per la protezione dei dati personali 2016/679 (General Data Protection Regulation o GDPR) è la fonte normativa principale in materia di protezione dei dati personali. Pubblicato nella Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018 (D. Lgs. di adeguamento 101 del 2018).

Come si è preparata l'Italia all'applicazione del Regolamento? La L. 25 ottobre 2017, n. 163 delega il Governo ad emanare uno o più decreti legislativi con i quali adeguare le norme nazionali alle disposizioni del regolamento, modificando o abrogando quelle incompatibili. Il Garante, in attuazione delle disposizioni della L. 205/2017, ha pubblicato il 22 febbraio il Provvedimento n. 121 per fornire le indicazioni preliminari per la corretta applicazione del Regolamento. Il 19 aprile il Garante privacy fornisce un ulteriore chiarimento sul provvedimento e precisa che con il provvedimento non sono state differite le funzioni ispettive e sanzionatorie in capo al Garante e conferma la data del 25 maggio 2018 per l'entrata in vigore del Regolamento. In attuazione della delega, il 4 settembre 2018 è stato pubblicato sulla Gazzetta Ufficiale il D. Lgs. 10 agosto 2018, n. 101 contenente le disposizioni per l'adeguamento della normativa nazionale al GDPR. Il D. Lgs. 101/2018, che ha modificato profondamente il D. Lgs. 196/2003, di fatto riconosce nel GDPR la norma di rango primario a cui tutti i soggetti, pubblici e privati, che intendano trattare dati personali devono fare riferimento (era necessario? N.d.a.). Tale indicazione obbliga tutte le pubbliche amministrazioni (tra cui anche le istituzioni scolastiche) a rivedere tutto il sistema di gestione della protezione dei dati personali e a farsi carico di una serie di adempimenti obbligatori finalizzati ad implementare la sicurezza dei dati, sulla base del principio della responsabilizzazione (accountability) dei soggetti titolari del trattamento dei dati.

IL CODICE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI (CODICE DELLA PRIVACY - c.d.p.). Il Codice si caratterizza per il riconoscimento di una serie di diritti alle persone fisiche (inizialmente anche alle persone giuridiche) relativamente ai propri dati.

Principi generali per l'attività di trattamento

Art. 2 Cost. → il trattamento deve avvenire assicurando la tutela dei diritti e delle libertà fondamentali.
L'esercizio del trattamento deve avvenire mediando tra la tutela dei diritti e delle libertà fondamentali ed una serie di principi che già sono stati positivizzati con la L. 241/1990 e che devono improntare tutta l'azione amministrativa.
a) Dato personale → "qualunque informazione" relativa a persona fisica, identificata o identificabile, anche indirettamente, mediante riferimento a qualsiasi altra informazione, ivi compreso un numero di identificazione personale (numero di telefono, indirizzo, impronte digitali, immagine ecc.). Art. 4 → diverse tipologie che rientrano nella categoria generale di dato personale:
1 - dati identificativi: permettono l'identificazione diretta del soggetto, mentre è considerato dato anonimo quel dato che non è collegabile ad alcun soggetto;
2 - dati sensibili e ultra-sensibili: sono quei dati personali idonei a rivelare l'origine razziale ed etnica, le convinzioni religiose, filosofiche, le opinioni politiche, l'adesione a partiti, sindacati, associazioni, nonché i dati personali idonei a rivelare lo stato di salute e la vita sessuale;
3 - dati giudiziari che sono quei dati personali idonei a rivelare informazioni personali in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi del codice di procedura penale. 705
b) Trattamento dei dati (art. 4) → qualunque operazione effettuata, concernenti la raccolta, la registrazione, l'organizzazione, la conservazione, l'elaborazione, la diffusione, la cancellazione … di dati. Anche il compimento di una sola delle operazioni anzidette configura un'ipotesi di trattamento.
IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI. E' l'"arbitro" delle situazioni controverse, assicura la corretta applicazione delle relative disposizioni → autorità amministrativa indipendente → autonomia e indipendenza di giudizio.
I compiti principali del Garante sono:
controllare che i trattamenti di dati personali siano conformi alla disciplina e prescrivere le misure da adottare;
esaminare reclami e segnalazioni nonché decidere i ricorsi presentati dagli interessati o dalle associazioni;
vietare il trattamento illecito o non corretto dei dati, ovvero disporre il blocco del trattamento di dati personali;
adottare i provvedimenti previsti dalla normativa in materia di dati personali (es. autorizzazioni per il trattamento dei dati sensibili);
promuovere la sottoscrizione dei codici di deontologia e di buona condotta in vari ambiti (credito al consumo, attività giornalistica);
segnalare al Parlamento e al Governo l'opportunità di adottare provvedimenti normativi specifici;
esprimere pareri nei casi previsti, in particolare quando richiesti dal Presidente del Consiglio o da ciascun ministro in ordine a regolamenti ed atti amministrativi;
relazione annuale da trasmettere al Parlamento e al Governo;
curare la tenuta del registro dei trattamenti, formato sulla base delle notificazioni di trattamento ricevute;
curare l'informazione dei cittadini in materia di trattamento dei dati personali, nonché sulle misure di sicurezza;

coinvolgere i cittadini con consultazioni pubbliche;
denunciare i fatti configurabili come reati perseguibili d'ufficio.
Il legislatore ha attribuito al Garante una serie di poteri, ispettivi, di controllo e sanzionatori. L'art. 157 c.d.p. disciplina un potere di vigilanza e controllo che il Garante esercita a seguito di segnalazioni. Il Garante può richiedere ai soggetti coinvolti nel trattamento dei dati - al titolare, al responsabile, all'interessato e a terzi - di fornire informazioni. Accertamenti ispettivi → effettuati in collaborazione con le Unità Speciali della Guardia di Finanza - Nucleo Speciale Privacy.
Quanto ai poteri sanzionatori, il Codice distingue tra violazioni amministrative e illeciti penali. Quanto al primo aspetto, a titolo di esempio, si ricorda la previsione dell'art. 161: si tratta del caso di omissione o inidoneità dell'informativa che deve essere resa all'interessato in ordine al trattamento dei propri dati personali, al fine di ottenere il consenso allo stesso → sanzione pecuniaria da un minimo di 6 mila euro ad un massimo di 36 mila euro.
TITOLARE, RESPONSABILE E INCARICATO DEL TRATTAMENTO. Titolare del trattamento → colui che effettua il trattamento e che ha potere decisionale autonomo in ordine alle finalità, alle modalità del trattamento e agli strumenti da utilizzare, compreso il profilo della sicurezza.
Il titolare del trattamento può nominare un responsabile del trattamento dei dati, attribuendogli una serie di compiti analiticamente determinati, per iscritto, nell'atto di nomina. La nomina del responsabile è facoltativa. Il responsabile effettua il trattamento attenendosi alle istruzioni impartite dal titolare il quale vigila. Il responsabile del trattamento deve godere di un'esperienza, di una capacità e di un'affidabilità tali da soddisfare le esigenze di pieno rispetto delle vigenti disposizioni in materia e se le necessità organizzative lo richiedano, il titolare può designare come responsabili più soggetti, provvedendo anche alla suddivisione dei compiti.
Indispensabile è l'individuazione degli incaricati del trattamento, ossia delle persone autorizzate a compiere operazioni di trattamento dal titolare o dal responsabile → sotto la diretta autorità del titolare o del responsabile, attenendosi alle istruzioni impartite, e la cui designazione sia stata effettuata per iscritto con puntuale individuazione dell'ambito del trattamento consentito. La designazione è comunque valida quando, pur non essendo espressa per la singola persona, consiste nella documentata preposizione della persona fisica ad un'unità organizzativa per la quale sia già stato individuato, per iscritto, l'ambito del trattamento consentito agli addetti preposti alla stessa.
Il titolare del trattamento dei dati personali nell'istituzione scolastica è il DS, in quanto suo rappresentante legale.
Egli può designare il responsabile del trattamento dei dati personali che è, innanzitutto, il DSGA. In subordine, il DS può affidare l'incarico ad altra figura professionale, anche esterna.
In relazione ai dati personali che riguardano i loro studenti, gli insegnanti devono essere informati del trattamento, soprattutto se si tratta di dati sensibili da trattare per la redazione di Piani didattici individualizzati (ad es. certificazioni mediche), di scelte relative all'insegnamento della religione, di diete per motivi di salute ecc. Con la nuova normativa sulla trasparenza (D. Lgs. 33/2013) → linee guida 2014 contemperare le esigenze di pubblicità e trasparenza con i diritti e le libertà fondamentali delle persone. Le Linee Guida riguardano la pubblicazione di atti che

le P.A. devono mettere online per finalità di trasparenza (obblighi di pubblicità). Per garantire la trasparenza online, il Garante ha previsto:
la pubblicazione esclusivamente di dati esatti, aggiornati, pertinenti e non eccedenti rispetto allo scopo della pubblicazione;
la possibilità del riutilizzo dei dati pubblicati (ad esclusione dei dati sensibili e giudiziari) solo per scopi per i quali i dati stessi sono stati raccolti e nel rispetto del norme sulla privacy;
con riferimento alla durata degli obblighi di pubblicazione, l'oscuramento dei dati pubblicati online anche prima dello spirare del termine di 5 anni previsto dal D.Lgs. 33/2013, una volta che siano stati raggiunti gli scopi.
L'INTERESSATO. Art. 4 → "la persona fisica, cui si riferiscono i dati personali". L'interessato, quale dominus del dato personale, ha il potere di incidere sul trattamento da realizzare, attraverso l'esercizio di una serie di pretese → diritto ad ottenere la conferma dell'esistenza o meno di dati personali che lo riguardano e la loro comunicazione in forma intelligibile. Inoltre, ha il diritto di ottenere l'indicazione:
dell'origine dei propri dati personali;
delle finalità e delle modalità del loro trattamento;
della logica applicata al trattamento con strumenti elettronici;
degli estremi identificativi del titolare, dei responsabili e del rappresentante designato a norma di L.;
dei soggetti ai quali i dati personali possono essere comunicati.
L'interessato, infine, ha il diritto di opporsi, purché per motivi legittimi, al trattamento dei dati personali.
Per l'esercizio dei propri diritti, è sufficiente presentare una richiesta, che deve essere riscontrata, senza ritardo, da chi effettua il trattamento → mediante lettera raccomandata, telefax o posta elettronica o ulteriori soluzioni tecnologiche. Art. 10 → modalità con cui è possibile evadere una richiesta. Il legislatore impone al titolare l'obbligo di agevolare l'accesso ai dati personali da parte dell'interessato e l'obbligo di semplificare le modalità per effettuare il riscontro (uffici per le relazioni con il pubblico). SaLgs. che la richiesta sia circoscritta, il riscontro alla stessa comprende tutti i dati personali che riguardano l'interessato. I dati sono estratti (dal responsabile o dall'incaricato) e possono essere comunicati al richiedente anche oralmente. Se vi è richiesta, si provvede alla trasposizione dei dati su supporto cartaceo o informatico, ovvero alla loro trasmissione per via telematica. L'effettività della tutela degli interessati è garantita anche dall'obbligo di comunicare i dati in forma intelligibile (grafia comprensibile). Il riscontro alle richieste di accesso deve essere effettuato senza ritardo (art. 8) e comunque non oltre 15 giorni dal ricevimento della richiesta.
AMMINISTRATORE DI SISTEMA. Gli "amministratori di sistema" sono figure essenziali per la sicurezza delle banche dati e la corretta gestione delle reti telematiche. Sono esperti chiamati a svolgere delicate funzioni che comportano la concreta capacità di accedere a tutti i dati che transitano sulle reti aziendali ed istituzionali. Ad essi viene affidato spesso anche il compito di vigilare sul corretto utilizzo dei sistemi informatici di un'azienda o di una pubblica amministrazione. Per questo il Garante ha prescritto l'adozione di specifiche misure tecniche ed organizzative che agevolino la verifica sulla sua attività da parte di chi ha la titolarità delle banche dati e dei sistemi informatici.

Criteri per l'individuazione. Nomina da parte del titolare del trattamento dopo attenta valutazione di esperienza, capacità, e affidabilità della persona chiamata a ricoprire il ruolo di amministratore che deve essere in grado di garantire il pieno rispetto della normativa in materia di protezione dei dati personali, compreso il profilo della sicurezza.
Registrazione degli accessi. Adozione di sistemi di controllo che consentano la registrazione degli accessi effettuati dagli amministratori di sistema ai sistemi di elaborazione e agli archivi elettronici. Le registrazioni devono comprendere i riferimenti temporali e la descrizione dell'evento che le ha generate e devono essere conservate per un congruo periodo, non inferiore a sei mesi.
Verifica della attività. Verifica almeno annuale da parte dei titolari del trattamento sulla rispondenza dell'operato degli amministratori di sistema alle misure organizzative, tecniche e di sicurezza previste dalla L. per i trattamenti di dati personali.
Estremi identificativi. Il Garante ha previsto che gli estremi identificativi e l'elenco delle funzioni attribuite all'amministratore di sistema siano indicati nel DPS (oggi non più obbligatorio) o in un documento interno disponibile in caso di accertamenti da parte del Garante.
INFORMATIVA ALL'INTERESSATO. Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. L'interessato o la persona presso la quale sono raccolti i dati personali sono previamente informati oralmente o per iscritto circa:

a) le finalità e le modalità del trattamento cui sono destinati i dati;
b) la natura obbligatoria o facoltativa del conferimento dei dati;
c) le conseguenze di un eventuale rifiuto di rispondere;
d) i soggetti o le categorie di soggetti ai quali i dati personali possono essere comunicati o che possono venirne a conoscenza in qualità di responsabili o incaricati, e l'ambito di diffusione dei dati medesimi;
e) i diritti riconosciuti dalla normativa (diritto di accesso, diritto di aggiornare i dati, ecc.);
f) gli estremi identificativi del titolare e, se designati, del rappresentante nel territorio dello Stato ai sensi dell'art. 5 e del responsabile. Quando il titolare ha designato più responsabili è indicato almeno uno di essi, indicando il sito della rete di comunicazione o le modalità attraverso le quali è conoscibile in modo agevole l'elenco aggiornato dei responsabili. Quando è stato designato un responsabile per il riscontro all'interessato in caso di esercizio dei diritti di cui all'art. 7, è indicato tale responsabile.

I PRINCIPI APPLICABILI AL TRATTAMENTO
Due regole fondamentali:
a) *la strumentalità del trattamento rispetto al perseguimento dei fini istituzionali dell'ente* → svolgimento delle funzioni istituzionali;
b) *il divieto di acquisire il consenso dell'interessato al trattamento*: la più importante distinzione rispetto alla disciplina prevista per i privati è rappresentata dal fatto che i soggetti pubblici per effettuare il trattamento «non devono richiedere il consenso dell'interessato». Tale regola non trova applicazione per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici.

DATI PERSONALI COMUNI. Il trattamento dei “dati diversi da quelli sensibili e giudiziari” è consentito anche in mancanza di una norma di L. o di regolamento che espressamente lo contempli, sempreché lo stesso sia effettuato perseguendo finalità istituzionali.
Si distingue, inoltre, il trattamento chiuso dal trattamento aperto: il primo si realizza quando il trattamento rimane all'interno dell'entità nel suo complesso. Il trattamento chiuso è lecito se risponde ad esigenze di ufficio riferite alle competenze delle singole unità organizzative. Il secondo, invece, si verifica quando sono coinvolti soggetti esterni all'amministrazione, per cui «il dato personale esce dalla sfera di un titolare del trattamento per essere trasferito ad altro titolare di trattamento».
La comunicazione di dati personali “comuni” da parte di un soggetto pubblico ad un altro soggetto pubblico è agevolata dal legislatore che la considera lecita se prevista da una norma di L. o di regolamento o se necessaria per lo svolgimento di funzioni istituzionali, e può essere iniziata solo se è decorso il termine di 45 giorni dal ricevimento della comunicazione al Garante prevista dall'art. 39 del Codice.
La comunicazione di dati personali “comuni”, da parte di un soggetto pubblico a privati o a enti pubblici economici e la diffusione degli stessi da parte di un soggetto pubblico è intesa in senso più restrittivo in quanto è ammessa esclusivamente sulla base di una norma di L. o di un regolamento.
DATI PERSONALI SENSIBILI E GIUDIZIARI. A differenza di quanto stabilito per i dati comuni, il cui trattamento è considerato lecito col solo richiamo alle funzioni istituzionali della P.A., per il trattamento dei dati sensibili l'art. 20 dispone che è consentito solo se autorizzato da espressa disposizione di L. (e non anche di regolamento come richiesto per il trattamento dei dati comuni) o da un provvedimento del Garante che specifichi:
le tipologie di dati che possono essere trattati (ad es. quello sanitario, quello attinente all'orientamento politico etc.);
le operazioni eseguibili (es. elaborazione, comunicazione etc.);
le finalità di rilevante interesse pubblico perseguite tra cui le finalità assistenziali e sociali (art. 73 c.d.p.) e l'istruzione in ambito scolastico, professionale o universitario (art. 95 c.d.p.).
IL TRATTAMENTO DEI DATI SENSIBILI E GIUDIZIARI EFFETTUATO DAL MIUR (D.M. 7 dicembre 2007, n. 305 «Regolamento relativo al trattamento dei dati sensibili e giudiziari nel settore dell'istruzione»). Il Regolamento individua nelle sette schede allegate gli ambiti dei dati trattati nelle scuole. Queste le schede:
Scheda 1: Selezione, reclutamento, rapporto di lavoro
Scheda 2: Gestione del contenzioso e procedimenti disciplinari
Scheda 3: Organismi collegiali e commissioni istituzionali
Scheda 4: Attività propedeutiche all'avvio dell'anno scolastico
Scheda 5: Attività educativa, didattica, formativa e di valutazione
Scheda 6: Scuole non statali
Scheda 7: Rapporti scuola-famiglia: gestione del contenzioso.
Ogni scheda consente alle scuole di individuare i trattamenti leciti evidenziando anche le finalità di rilevante interesse pubblico perseguite; le schede forniscono anche riferimenti riguardo alle fonti normative, ai soggetti esterni pubblici e privati a cui è possibile comunicare i dati, ai tipi di dati trattati. Ogni scheda, quindi, rappresenta una “guida” obbligatoria per le scuole.

Per effetto del Regolamento è necessario che alcuni atti e taluni procedimenti relativi ai dati sensibili siano modificati (ad esempio, il Documento Programmatico per la Sicurezza).
Il DS, nella qualità di titolare del trattamento, deve adeguare la nomina del Responsabile del trattamento informandolo anche delle prescrizioni contenute nel Regolamento. La L. 107/2015 (commi 136-144) istituisce il Portale Unico dei dati della scuola relativi al sistema di istruzione, attraverso il quale il MIUR garantisce l'accesso e la riutilizzabilità dei dati delle scuole. In esso confluiranno fra l'altro:
dati relativi al curriculum dello studente, condivisi con le scuole;
dati relativi al fascicolo di ciascun docente;
bilanci di ciascuna scuola:
dati del Sistema nazionale di valutazione;
normativa;
Anagrafe dell'edilizia scolastica;
Anagrafe degli studenti;
Piani triennali dell'offerta formativa;
incarichi di docenza.
Il c. 140 stabilisce che il sistema non può richiedere alle scuole dati già comunicati o già presenti nel Portale Unico.
DECRETO MINISTERIALE N.305 DEL 7.12.2006, REGOLAMENTO RECANTE IDENTIFICAZIONE DEI DATI SENSIBILI E GIUDIZIARI TRATTATI E DELLE RELATIVE OPERAZIONI EFFETTUATE DAL MINISTERO DELLA PUBBLICA ISTRUZIONE. Il Regolamento completa il quadro normativo relativo al diritto alla protezione dei dati personali ed alla riservatezza definito dal codice emanato con il D. Lgs. 196 del 30 giugno 2003.
Nella scuola abbiamo si dovrebbe provvedere a dare attuazione al Codice per quanto riguarda le autorizzazioni al trattamento dei dati personali al personale coinvolto, attraverso gli incarichi conferiti al personale docente da parte del DS ed al personale ATA (assistenti amministrativi e collaboratori scolastici) da parte del Responsabile del trattamento (DSGA); ogni incarico deve essere corredato da linee guida contente istruzioni per il trattamento e la protezione dei dati, deve essere fornita l'informativa dei diritti ai soggetti interessati (personale, alunni e genitori e fornitori), devono essere definite, applicate e monitorate le misure minime di sicurezza dei dati, deve essere stilato il Documento Programmatico sulla sicurezza.
Sono parte integrante del Regolamento 7 schede che individuano tutti i dati sensibili e giudiziari trattati dalle scuole, suddividendoli in 6 macro-categorie (ambiti):
Scheda n. 1 – Selezione e reclutamento a TI e TD e gestione del rapporto di lavoro;
Scheda n. 2 – Gestione del contenzioso e procedimenti disciplinari;
Scheda n. 3 – Organismi collegiali e commissioni istituzionali;
Scheda n. 4 – Attività propedeutiche all'avvio dell'anno scolastico;
Scheda n. 5 – Attività educativa, didattica e formativa e di valutazione;
Scheda n. 6 – Scuole non statali (relativamente agli eventuali dati sensibili e giudiziari che emergono nell'attività di vigilanza e controllo effettuata dall'Amministrazione e dai dirigenti scolastici delle scuole primarie incaricati della vigilanza sulle scuole non statali autorizzate);
Scheda n. 7 – Rapporti Scuola-Famiglie: gestione del contenzioso.

In particolare nella scheda n.4 relativa alle “Attività propedeutiche all’avvio dell’anno scolastico” si precisa che i dati sono forniti dagli alunni e dalle famiglie ai fini della frequenza dei corsi di studio nelle istituzioni scolastiche di ogni ordine e grado. Nell‘espletamento delle attività propedeutiche all‘avvio dell‘anno scolastico da parte delle istituzioni scolastiche, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche, per favorire l‘integrazione degli alunni con cittadinanza non italiana; alle convinzioni religiose, per garantire la libertà di credo religioso e per la fruizione dell‘insegnamento della religione cattolica o delle attività alternative a tale insegnamento;
- allo stato di salute, per assicurare l’erogazione del sostegno agli alunni diversamente abili e per la composizione delle classi;
- alle vicende giudiziarie, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- i dati giudiziari emergono anche nel caso in cui l’autorità giudiziaria abbia predisposto un programma di protezione nei confronti dell‘alunno nonché nei confronti degli alunni che abbiano commesso reati.

Nella scheda n. 5 relativa alla “Attività educativa. didattica e formativa, di valutazione” si precisa che nell’espletamento delle attività educative, didattiche e formative, curriculari ed extracurriculari, di valutazione ed orientamento, di scrutini ed esami, da parte delle istituzioni scolastiche di ogni ordine e grado, possono essere trattati dati sensibili relativi:

- alle origini razziali ed etniche per favorire l’integrazione degli alunni con cittadinanza non italiana;
- alle convinzioni religiose per garantire la libertà di credo religioso;
- allo stato di salute, per assicurare 1‘erogazione del servizio di refezione scolastica, del sostegno agli alunni disabili, dell‘insegnamento domiciliare ed ospedaliero nei confronti degli alunni affetti da gravi patologie, per la partecipazione alle attività educative e didattiche programmate, a quelle motorie e sportive, alle visite guidate e ai viaggi di istruzione;
- ai dati giudiziari, per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione;
- alle convinzioni politiche, per la costituzione e il funzionamento delle Consulte e delle Associazioni degli studenti e dei genitori,

I dati sensibili possono essere trattati per le attività di valutazione periodica e finale, per le attività di orientamento e per la compilazione della certificazione delle competenze.

Ogni scheda consente alle scuole di individuare chiaramente i trattamenti consentiti, le finalità di rilevante interesse pubblico perseguite, le fonti normative, i soggetti esterni pubblici e privati a cui è possibile comunicare i dati, i tipi di dati trattati e le tipologie più ricorrenti di trattamento.

Nel Documento Programmatico per la Sicurezza della scuola la sezione relativa all’elenco dei dati personali trattati (punto 19.1 del Disciplinare tecnico) sarà adeguata alle prescrizioni e indicazioni contenute nelle schede.

Gli incarichi del DS, relativi al personale docente, saranno consegnati individualmente. L’informativa agli interessati verrà effettuata nuovamente facendo riferimento alle prescrizioni del Regolamento e la diffusione della sua conoscenza,

effettuata fra i docenti con la presente comunicazione, sarà oggetto di una specifica occasione di formazione per il personale ATA incaricato.
Tutti i docenti hanno l'obbligo di prendere visione del Documento Programmatico per la Sicurezza e attenersi ad esso. Il Documento è affisso all'albo e pubblicato sul sito della scuola.
GARANTE PER LA PROTEZIONE DEI DATI PERSONALI «LINEE GUIDA IN MATERIA DI TRATTAMENTO DI DATI PERSONALI, CONTENUTI ANCHE IN ATTI E DOCUMENTI AMMINISTRATIVI, EFFETTUATO PER FINALITÀ DI PUBBLICITÀ E TRASPARENZA SUL WEB DA SOGGETTI PUBBLICI E DA ALTRI ENTI OBBLIGATI» (Allegato alla deliberazione n. 243 del 15 maggio 2014).
Dato personale: qualunque informazione relativa a persona fisica identificata o identificabile mediante qualsiasi informazione, ivi compreso un numero di identificazione personale.
Verifica prima della pubblicazione: prima della pubblicazione di un documento che contiene dati personali sul web, i soggetti pubblici devono verificare l'esistenza di una specifica norma di L. o di regolamento che preveda tale pubblicazione. La diffusione di dati comuni è ammessa solo se prevista da una norma di L. o di regolamento, mentre la diffusione di dati sensibili o giudiziari è ammessa se prevista espressamente solo da una norma di L..

a) Se non esiste una norma di L. o di regolamento che impone la pubblicazione nel sito istituzionale, la pubblicazione è legittima solo procedendo all'anonimizzazione dei dati personali.
b) Se esiste una norma di L. o di regolamento che ammette la pubblicazione nel sito istituzionale, i soggetti pubblici devono distinguere la natura dei dati personali oggetto di diffusione:
    a. dati comuni (es. nome e cognome, sesso, data e luogo di nascita, indirizzo, codice fiscale): si applica il principio di pertinenza e non eccedenza, i soggetti pubblici non possono rendere intellegibili i dati personali non necessari, eccedenti o non pertinenti con le finalità della pubblicazione;
    b. dati sensibili e giudiziari (dati sensibili: idonei a rivelare origine razziale ed etnica, convinzioni religiose, filosofiche o di altro genere, opinioni politiche, adesione a partiti, sindacati, associazioni e organizzazioni a carattere filosofico, politico o sindacale; dati giudiziari: idonei a rivelare provvedimenti di cui all'art. 3, co. 1, lett. da a) a o) e da r) a u), del d.P.R. 313/2002 in materia di casellario giudiziale, di anagrafe delle sanzioni amministrative dipendenti da reato e dei relativi carichi pendenti, o la qualità di imputato o di indagato ai sensi degli art. 60 e 61 del c.p.c.): possono essere diffusi solo se indispensabili per raggiungere le finalità della pubblicazione.;
    c. dati sensibili idonei a rivelare lo stato di salute: divieto assoluto di diffusione;
    d. dati sensibili idonei a rivelare la vita sessuale: divieto assoluto di diffusione per finalità di trasparenza. Per altre finalità possono essere diffusi solo se indispensabili.

Pubblicazione di dati personali ulteriori: le pubbliche amministrazioni non sono libere di diffondere «dati personali» ulteriori, non individuati dal d. lgs. n. 33/2013 o da altra specifica norma di L. o di regolamento (art. 19, c. 3, del Codice).
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» (art. 4, c. 3, del d. lgs. n. 33/2013).
Modalità di pubblicazione online dei dati personali (art. 7 del d. lgs. n. 33/2013). L'art. 7 del d. lgs. n. 33/2013 prevede che «I documenti, le informazioni e i dati oggetto di pubblicazione obbligatoria ai sensi della normativa vigente, resi disponibili anche a seguito dell'accesso civico di cui all'art. 5, sono pubblicati in formato di tipo aperto ai sensi dell'art. 68 del Codice dell'amministrazione digitale, di cui al D. Lgs. 7 marzo 2005, n. 82, e sono riutilizzabili ai sensi del D. Lgs. 24 gennaio 2006, n. 36, del D. Lgs. 7 marzo 2005, n. 82, e del D. Lgs. 30 giugno 2003, n. 196, senza ulteriori restrizioni diverse dall'obbligo di citare la fonte e di rispettarne l'integrità». La disposizione citata persegue, peraltro, lo scopo di non obbligare gli utenti a dotarsi di programmi proprietari o a pagamento per la fruizione – e, quindi, per la visualizzazione – dei file contenenti i dati oggetto di pubblicazione obbligatoria. Infatti, il «formato di tipo aperto» è «un formato di dati reso pubblico, documentato esaustivamente e neutro rispetto agli strumenti tecnologici necessari per la fruizione dei dati stessi» (art. 68, c. 3, lett. a), del d. lgs. 7 marzo 2005, n. 82, Codice dell'amministrazione digitale-CAD).
Durata degli obblighi di pubblicazione. L'art. 8, c. 3, del d. lgs. n. 88/2013 prevede che i dati, le informazioni e i documenti oggetto di pubblicazione «sono pubblicati per un periodo di 5 anni, decorrenti dal 1° gennaio dell'anno successivo a quello da cui decorre l'obbligo di pubblicazione, e comunque fino a che gli atti pubblicati producono i loro effetti, fatti salvi i diversi termini previsti dalla normativa in materia di trattamento dei dati personali e quanto previsto dagli articoli 14, c. 2, e 15, c. 4».
Indicizzazione tramite motori di ricerca. L'art. 9 del d. lgs. n. 33/2013 stabilisce che «Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione "Amministrazione trasparente"».
Obblighi di pubblicazione dei curricula professionali (art. 10, c. 8, lett. d), del d. lgs. n. 33/2013 et al.). La disciplina in materia di trasparenza prevede di rendere visibile al pubblico, rispetto a taluni soggetti, informazioni personali concernenti il percorso di studi e le esperienze professionali rilevanti, nella forma del curriculum redatto in conformità al vigente modello europeo (art. 10, c. 8, lett. d)). Le ipotesi previste riguardano, ad esempio, i curricula professionali dei titolari di incarichi di indirizzo politico (art. 14), dei titolari di incarichi amministrativi di vertice, dirigenziali e di collaborazione o consulenza (art. 15, c. 1, lett. b), nonché delle posizioni dirigenziali attribuite a persone – anche esterne alle pubbliche amministrazioni – individuate discrezionalmente dall'organo di indirizzo politico senza procedure pubbliche di selezione, di cui all'art. 1, commi 39 e 40, della L. 6 novembre 2012, n. 190 (art. 15, c. 5), dei componenti degli organismi indipendenti di valutazione (art. 10, c. 8, lett. c), nonché dei dirigenti in ambito sanitario come individuati dall'art. 41, commi 2 e 3.
Il riferimento del legislatore all'obbligo di pubblicazione del curriculum non può tuttavia comportare la diffusione di tutti i contenuti astrattamente previsti dal modello europeo (rispondendo taluni di essi alle diverse esigenze di favorire l'incontro tra

domanda e offerta di lavoro in vista della valutazione di candidati), ma solo di quelli pertinenti rispetto alle finalità di trasparenza perseguite.
Prima di pubblicare sul sito istituzionale i curricula, il titolare del trattamento dovrà pertanto operare un'attenta selezione dei dati in essi contenuti, se del caso predisponendo modelli omogenei e impartendo opportune istruzioni agli interessati (che, in concreto, possono essere chiamati a predisporre il proprio curriculum in vista della sua pubblicazione per le menzionate finalità di trasparenza). In tale prospettiva, sono pertinenti le informazioni riguardanti i titoli di studio e professionali, le esperienze lavorative (ad es., gli incarichi ricoperti), nonché ulteriori informazioni di carattere professionale (si pensi alle conoscenze linguistiche oppure alle competenze nell'uso delle tecnologie, come pure alla partecipazione a convegni e seminari oppure alla redazione di pubblicazioni da parte dell'interessato).
Non devono formare invece oggetto di pubblicazione dati eccedenti, quali ad esempio i recapiti personali oppure il codice fiscale degli interessati, ciò anche al fine di ridurre il rischio di c.d. furti di identità.
Deve inoltre essere garantita agli interessati la possibilità di aggiornare periodicamente il proprio curriculum ai sensi dell'art. 7 del Codice evidenziando gli elementi oggetto di aggiornamento.
Evitare la duplicazione massiva dei file contenenti dati personali. Devono essere adottate opportune cautele per ostacolare operazioni di duplicazione massiva dei file contenenti dati personali da parte degli utenti della rete, rinvenibili sui siti istituzionali delle amministrazioni pubbliche, mediante l'utilizzo di software o programmi automatici, al fine di ridurre il rischio di riproduzione e riutilizzo dei contenuti informativi in ambiti e contesti differenti. A tale scopo si può fare ricorso ad accorgimenti consistenti, ad esempio, nell'uso di strumenti tecnologici in grado di riconoscere accessi che risultino anomali per la loro frequenza o perché realizzati tramite l'azione di strumenti automatizzati e non da persone: si può ricorrere in tal caso a sistemi di verifica 'captcha'.
Graduatorie. Con riguardo alla pubblicità degli esiti delle prove concorsuali e delle graduatorie finali – nonché, nei casi (e con le modalità) previsti, dei risultati di prove intermedie – di concorsi e selezioni pubbliche e di altri procedimenti che prevedono la formazione di graduatorie, restano salve le normative di settore che ne regolano tempi e forme di pubblicità (ad es., affissione presso la sede dell'ente pubblico, pubblicazione nel bollettino dell'amministrazione o, per gli enti locali, all'albo pretorio). Tale regime di conoscibilità, assolve alla funzione di rendere pubbliche le decisioni adottate dalla commissione esaminatrice e/o dall'ente pubblico procedente, anche al fine di consentire agli interessati l'attivazione delle forme di tutela dei propri diritti e di controllo della legittimità delle procedure concorsuali o selettive. Anche a questo riguardo devono essere diffusi i soli dati pertinenti e non eccedenti riferiti agli interessati. Non possono quindi formare oggetto di pubblicazione dati concernenti i recapiti degli interessati (si pensi alle utenze di telefonia fissa o mobile, l'indirizzo di residenza o di posta elettronica, il codice fiscale, l'indicatore Isee, il numero di figli disabili, i risultati di test psicoattitudinali o i titoli di studio), né quelli concernenti le condizioni di salute degli interessati (cfr. art. 22, c. 8, del Codice), ivi compresi i riferimenti a condizioni di invalidità, disabilità o handicap fisici e/o psichici.

GLI INTERVENTI DEL GARANTE IN MATERIA DI PROTEZIONE DEI DATI PERSONALI NELLE SCUOLE. Il Garante ha più volte fornito ulteriori chiarimenti per le scuole; tali chiarimenti sono stati accolti in una guida resa disponibile sul sito del MIUR. Le scuole devono, in primo luogo, rendere noti alle famiglie e ai ragazzi, attraverso un'adeguata informativa, i dati che raccolgono e le modalità di utilizzo degli stessi. Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte o incomplete.

LA SCUOLA DEVE RENDERE L'INFORMATIVA. Tutte le scuole – sia quelle pubbliche, sia quelle private – hanno l'obbligo di far conoscere agli "interessati" (studenti, famiglie, professori, etc.) come vengono trattati i loro dati personali. Devono cioè rendere noto – attraverso un'adeguata informativa con le modalità ritenute più opportune, eventualmente anche online – quali dati raccolgono, come li utilizzano e a quale fine.

ALCUNE SEMPLICI REGOLE PER IL PERSONALE SCOLASTICO.

Collaboratore scolastico. Custodisce i dati che gestisce, come ad esempio i numeri di telefono di studenti e dei lavoratori, chiusi a chiave nel cassetto della sua postazione; non parla fuori dai locali scolastici dei fatti riservati di studenti e lavoratori che conosce per esigenze di lavoro; se supporta la segreteria o i docenti, ad esempio si pensi al servizio fotocopie, mantiene la massima riservatezza sulle informazioni contenute nei documenti e sui dati personali.

Docenti. Usa una password personale e la tiene segreta verso tutti; mantiene riservate le password che utilizza per questioni di servizio (si pensi ad esempio alla password per accedere alla rete WiFi o al registro elettronico); cambia la password ogni 6 mesi; se si allontana dall'aula, blocca o spegne il proprio computer e quello eventualmente in dotazione alla classe; si preoccupa della adeguatezza e della custodia degli atti e dei verbali di propria competenza; usa chiavette USB criptate; non parla fuori da scuola di fatti riservati di studenti e lavoratori.

DS, DSGA e personale amministrativo. Usa una password personale e la tiene segreta verso tutti; mantiene riservate le password che utilizza per questioni di servizio (si pensi ad esempio alla password per accedere alla rete WiFi o al registro elettronico); cambia la password ogni 6 mesi; se si allontana dalla propria postazione, blocca o spegne il proprio computer e quello eventualmente in dotazione per questioni di servizio; si preoccupa della adeguatezza e della custodia degli atti e dei verbali di propria competenza; usa chiavette USB criptate; non parla fuori da scuola di fatti riservati di studenti e lavoratori; il DS designa il DPO e un tecnico che attui le misure informatiche necessarie; il DS redige, per il tramite del DPO, la documentazione obbligatoria; il DS organizza la formazione dei lavoratori; il DS e il DSGA vigilano sull'operato del personale scolastico.

È POSSIBILE ACCEDERE AI PROPRI DATI PERSONALI DETENUTI DAGLI ISTITUTI SCOLASTICI. Ogni persona ha diritto di conoscere se sono conservate informazioni che la riguardano, di farle rettificare se erronee o non aggiornate. Per esercitare questi diritti è possibile rivolgersi direttamente al "titolare del trattamento" (in genere l'istituto scolastico di riferimento). Se la scuola non risponde o il riscontro non è adeguato, è possibile rivolgersi al Garante o alla magistratura ordinaria.

IN CASO DI DELEGA PER PRELEVARE IL PROPRIO FIGLIO A SCUOLA, È NECESSARIO FORNIRE COPIA DELLA CARTA D'IDENTITÀ DEL DELEGANTE E DEL DELEGATO. Sulla base del principio generale di accountability, è facoltà delle

istituzioni scolastiche regolare e modulare tale modalità, assicurando al tempo stesso le cautele necessarie a garantire l'identificabilità dei soggetti coinvolti e che i dati eventualmente raccolti siano protetti (da accessi abusivi, rischi di perdita o manomissione) con adeguate misure di sicurezza.

GLI ESITI DEGLI SCRUTINI O DEGLI ESAMI DI STATO SONO PUBBLICI. Le informazioni sul rendimento scolastico sono soggette ad un regime di conoscibilità stabilito dal MIUR. E' preferibile che i risultati analitici siano pubblicati sulla sezione riservata del Registro elettronico accessibile solo agli studenti e ai genitori. Nel pubblicare i voti degli scrutini e degli esami nei tabelloni, l'istituto scolastico deve evitare, però, di fornire informazioni sulle condizioni di salute degli studenti o altri dati personali non pertinenti. Il riferimento alle "prove differenziate" sostenute, ad esempio, dagli studenti con disturbi specifici di apprendimento (DSA) non va inserito nei tabelloni, ma deve essere indicato solamente nell'attestazione da rilasciare allo studente.

LE SCUOLE POSSONO TRATTARE LE CATEGORIE PARTICOLARI DI DATI PERSONALI. Le scuole possono trattare le categorie particolari di dati personali (es. dati sulle convinzioni religiose, dati sulla salute) solo se espressamente previsto da norme di L. o regolamentari. In ogni caso non possono essere diffusi i dati relativi alla salute: non è consentito, ad esempio, pubblicare online una circolare contenente i nomi degli studenti con disabilità oppure quegli degli alunni che seguono un regime alimentare differenziato per motivi di salute.

NELLE COMUNICAZIONI SCUOLA-FAMIGLIA NON POSSONO ESSERE INSERITI DATI PERSONALI DEGLI ALUNNI. Nelle circolari, nelle delibere o in altre comunicazioni non rivolte a specifici destinatari non possono essere inseriti dati personali che rendano identificabili gli alunni (ad esempio, quelli coinvolti in casi di bullismo o quelli cui siano state comminate sanzioni disciplinari o interessati da altre vicende delicate).

I DATI DEGLI ALLIEVI DISABILI O CON DISTURBI SPECIFICI DELL'APPRENDIMENTO (DSA). La conoscenza di tali dati è limitata ai soli soggetti a ciò legittimati dalla normativa scolastica e da quella specifica di settore, come ad esempio i docenti, i genitori e gli operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato (L. n. 104/92, L. n. 328/2000 e D. Lgs. n. 66/2017).

L'UTILIZZO DEGLI SMARTPHONE. Spetta alle istituzioni scolastiche disciplinare l'utilizzo degli smartphone all'interno delle aule o nelle scuole stesse. In ogni caso, laddove gli smartphone siano utilizzati per riprendere immagini o registrare conversazioni, l'utilizzo dovrà avvenire esclusivamente per fini personali e nel rispetto dei diritti delle persone coinvolte.

È lecito registrare la lezione per scopi personali, ad esempio per motivi di studio individuale, compatibilmente con le specifiche disposizioni scolastiche al riguardo. Per ogni altro utilizzo o eventuale diffusione, anche su Internet, è necessario prima informare le persone coinvolte nella registrazione (professori, studenti…) e ottenere il loro consenso.

Gli allievi con DSA possono utilizzare liberamente strumenti didattici che consentano loro anche di registrare (c.d. "strumenti compensativi e aumentativi"). La specifica normativa di settore (L. n. 170/2010) prevede che gli studenti che presentano tali disturbi hanno il diritto di utilizzare strumenti di ausilio per una

maggiore flessibilità didattica. In particolare, viene stabilito che gli studenti con diagnosi DSA possono utilizzare gli strumenti di volta in volta previsti dalla scuola nei piani didattici personalizzati che li riguardano (ivi compreso il registratore o il pc). In questi casi non è necessario richiedere il consenso delle persone coinvolte nella registrazione.

GLI ISTITUTI SCOLASTICI POSSONO PUBBLICARE SUI PROPRI SITI INTERNET LE GRADUATORIE DI DOCENTI E PERSONALE ATA. Questo consente a chi ambisce a incarichi e supplenze di conoscere la propria posizione e il proprio punteggio. Tali liste devono però contenere solo il nome, il cognome, il punteggio e la posizione in graduatoria. È invece eccedente la pubblicazione dei numeri di telefono e degli indirizzi privati dei candidati.

SI POSSONO INSTALLARE TELECAMERE ALL'INTERNO DEGLI ISTITUTI SCOLASTICI. L'eventuale installazione di sistemi di videosorveglianza presso le scuole deve garantire il diritto dello studente alla riservatezza. Può risultare ammissibile l'utilizzo di tali sistemi in casi di stretta indispensabilità, al fine di tutelare l'edificio e i beni scolastici da atti vandalici, circoscrivendo le riprese alle sole aree interessate. È inoltre necessario segnalare la presenza degli impianti con cartelli. 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. Se le riprese riguardano l'esterno della scuola, l'angolo visuale delle telecamere deve essere opportunamente delimitato

LE SCUOLE POSSONO CONSENTIRE A SOGGETTI LEGITTIMATI DI SVOLGERE ATTIVITÀ DI RICERCA TRAMITE QUESTIONARI, DA SOTTOPORRE AGLI ALUNNI, CONTENENTI RICHIESTE DI INFORMAZIONI PERSONALI. Tali attività sono consentite solo se gli studenti e, nel caso di minori, chi esercita la responsabilità genitoriale, siano stati preventivamente informati sulle modalità di trattamento e sulle misure di sicurezza adottate per proteggere i dati personali degli alunni e, ove previsto, abbiano acconsentito al trattamento dei dati. Ragazzi e genitori devono, comunque, avere sempre la facoltà di non aderire all'iniziativa.

SCUOLE CHE PUBBLICATO FOTO, VIDEO E AUDIO DI MINORI: NON BASTA IL CONSENSO DA PARTE DEGLI ESERCENTI LA POTESTÀ GENITORIALE. In via preliminare va precisato che ai fini dell'applicazione della vigente normativa in materia di protezione dei dati personali (Regolamento UE 2016/679 – GDPR e D. Lgs. 196/2003 – Codice Privacy):

- le immagini e la voce sono informazioni che permettono l'identificazione diretta della persona interessata e sono pertanto da considerare "dati personali" a tutti gli effetti;
- costituisce "trattamento di dati" qualsiasi operazione compiuta con o sui dati personali (come ad esempio la raccolta, la conservazione, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, ecc.);
- anche la sola registrazione di video o foto che riprendono persone identificabili si configura come un "trattamento di dati personali", come tale assoggettabile alla citata normativa.

La questione relativa alla raccolta ed eventuale pubblicazione di foto e video in ambito scolastico è stata da tempo affrontata (e risolta) dall'Autorità Garante nei seguenti termini, con riguardo ad una ben definita fattispecie.

Alla FAQ: “Violano la privacy le riprese video e le fotografie raccolte dai genitori durante le recite, le gite e i saggi scolastici?” (https://www.garanteprivacy.it/home/faq/scuola-e-privacy), la risposta fornita dal Garante è negativa, perché “Le immagini, in questi casi, sono raccolte per fini personali e destinate a un ambito familiare o amicale.”
Il “via libera” che ne discende risulta subordinato al sussistere di queste quattro condizioni (enucleabili dalla stessa formulazione della domanda e della risposta):

I) deve evidentemente trattarsi di un evento in ambito scolastico che è aperto alla partecipazione dei genitori;
II) i soggetti autorizzati ad effettuare tali riprese sono i genitori;
III) la finalità da essi perseguita deve essere personale;
IV) l’ambito di circolazione dei dati personali raccolti (foto e video) deve limitarsi a quello familiare o amicale.

La risposta del Garante precisa inoltre che: “Va però prestata particolare attenzione alla eventuale pubblicazione delle medesime immagini su Internet e sui social network. In caso di diffusione di immagini dei minori diventa infatti indispensabile ottenere il consenso da parte degli esercenti la potestà genitoriale”.
In pratica, ferme le prime tre condizioni, se la quarta non è rispettata perché l’ambito di circolazione delle riprese si estende ad una platea più ampia di destinatari mediante pubblicazione via internet, è necessario acquisire il preventivo consenso dei genitori dei minori coinvolti.
Rispetto a questa indicazione fornita dal Garante, cosa cambia se – in diversa fattispecie – a fare le riprese video o raccogliere le fotografie degli alunni è il personale scolastico? Lo scenario è completamente diverso perché:

le riprese vengono verosimilmente effettuate in un contesto “chiuso”, che cioè non prevede la presenza di soggetti esterni all’amministrazione scolastica (genitori e parenti degli alunni, visitatori, ecc.);
è cambiata la qualità del soggetto che effettua le riprese (egli ha responsabilità del tutto diverse da quella genitoriale e quindi non può decidere per il minore);
è cambiata la finalità perseguita (non è più di tipo “personale” ma è semmai configurabile come “istituzionale”, “professionale”, “promozionale”, “motivazionale”, ecc.);
i dati personali raccolti non sono destinati a circolare in un ambito “familiare o amicale” (con ogni probabilità, essi costituiranno oggetto di comunicazione o diffusione mediante trasmissione telematica).

Date tali profonde differenze, non è possibile, in questa mutata prospettiva, continuare a fare affidamento sulla risposta del Garante che legittima (solo) il comportamento dei genitori.
In questo diverso caso, allo scopo di verificare la liceità del trattamento di dati che intende effettuare attraverso la ripresa di fotografie, audio o video di alunni, l’operatore scolastico dovrebbe porsi una serie di interrogativi preliminari progressivi:

La finalità del trattamento consiste nella esecuzione di un compito di interesse pubblico (o nell’adempimento di un obbligo legale)?
Il trattamento è funzionale al raggiungimento della finalità perseguita? (serve, ad esempio, per documentare l’attività formativa svolta nell’ambito di un P.O.N., o di un progetto didattico previsto nel P.T.O.F.)

Quel trattamento è l'unico modo per raggiungere la finalità perseguita? (non è possibile documentare diversamente l'attività svolta, ad esempio attraverso gli elaborati prodotti dagli alunni)

Il trattamento è proporzionato rispetto alla finalità perseguita? (i dati personali trattati sono ridotti al minimo indispensabile per il raggiungimento dello scopo)

La eventuale adozione di cautele particolari nel trattamento dei dati personali, tali da precludere la riconoscibilità dell'interessato (ad esempio riprendendo i soggetti di spalle o da lontano, evitando i primi piani, o pixellando i volti, ecc.), impedisce di raggiungere la finalità perseguita?

Se le risposte alle domande precedenti sono tutte affermative il trattamento può essere certamente considerato legittimo in sé, e non richiede la raccolta del preventivo consenso dei genitori.

Il consenso è invece assolutamente indispensabile se:

le domande precedenti hanno ricevuto risposte dubbie o addirittura negative (maggiore è il loro numero, maggiori possono essere le responsabilità che assume il titolare del trattamento);

i dati trattati sono destinati alla pubblicazione, cioè verranno messi a disposizione di soggetti indeterminati, ad esempio attraverso i canali social o il sito web (beninteso, al di fuori di circuiti protetti come può essere la piattaforma GPU per la gestione, il monitoraggio e la documentazione delle attività del Programma Operativo Nazionale, ed esclusi i casi in cui, per le particolari cautele adottate nel trattamento (vedi sopra sub 5) è stato spezzato il collegamento tra l'informazione personale pubblicata (immagine o voce) e l'interessato al quale essa appartiene).

In simili ipotesi, poiché il consenso dei genitori diventa la (necessaria e sufficiente) condizione di liceità del trattamento, è quanto mai opportuno che la questione venga attentamente ponderata dal titolare del trattamento (l'istituzione scolastica, in persona del suo Dirigente), effettuando di volta in volta un prudente bilanciamento di tutti gli interessi in gioco e dei potenziali rischi per l'interessato, tenendo in debito conto le considerazioni che seguono.

Per il principio di accountability stabilito dall'art. 24 del GDPR, il titolare del trattamento deve "garantire, ed essere in grado di dimostrare" la conformità del trattamento rispetto alla normativa vigente.

Il puntuale rispetto di tale obbligo di "rendicontazione" grava inevitabilmente la Scuola – nel caso dei trattamenti basati sul consenso – di oneri documentali, procedurali e di conservazione a causa della necessità di dover correttamente:

elaborare la formula ad hoc da sottoporre ai genitori, osservando i principi che presidiano la validità del consenso (adeguata informazione, anche in ordine alla revocabilità; forma "comprensibile e facilmente accessibile"; linguaggio semplice e chiaro; "granularità"; "chiara distinguibilità" da altre materie; ecc.);

gestire la fase della raccolta delle loro manifestazioni di volontà (verificandone in qualche modo la autenticità);

conservarle per il futuro, nell'evenienza di contestazioni;

procedere alla tempestiva cancellazione dei dati trattati qualora un genitore revochi il consenso in precedenza rilasciato (art. 17, par. 1, lett. b) del GDPR).

Laddove tali oneri vengano ritenuti accettabili (nell'interesse della Scuola), prima di procedere alla eventuale pubblicazione delle immagini di minori resta ancora da

valutare se – stabilito l'interesse superiore del fanciullo quale considerazione preminente (come prescrive la relativa Convenzione di New York del 1989) – i potenziali rischi che ne derivano risultano comunque giustificati.

PROTOCOLLO INFORMATICO, PROVVEDIMENTI DISCIPLINARI E PROTEZIONE DEI DATI PERSONALI DEI LAVORATORI. Il sistema di gestione dei documenti che utilizza il datore di lavoro non deve permettere agli altri dipendenti di conoscere di dati personali di altri dipendenti, in particolare relativi ai procedimenti disciplinari.

NON SI POSSONO PUBBLICARE SUL SITO DELLE SCUOLE I NOMI DEGLI STUDENTI DISTINTI PER CLASSE (AGOSTO 2020). Il Ministero dell'istruzione ritorna sul tema della privacy con una FAQ per il rientro a scuola a settembre. Non si possono pubblicare sul sito delle scuole i nomi degli studenti distinti per classe. La diffusione dei dati relativi alla composizione delle classi sul sito web istituzionale non è consentita in quanto, secondo l'art.2-ter del Codice in materia di protezione dei dati personali, la diffusione dei dati personali è lecita solo se disposta espressamente da una norma di L. o, nei casi previsti dalla L., di regolamento. Pertanto, le istituzioni scolastiche che intendano garantire in via preventiva la conoscibilità di tali dati dovranno utilizzare modalità idonee ad assicurare la tutela dei dati personali e i diritti degli interessati.

A tal fine i nominativi degli studenti distinti per classe potranno essere resi noti per le classi prime delle scuole di ogni ordine e grado, tramite apposita comunicazione all'indirizzo e-mail fornito dalla famiglia in fase di iscrizione all'a.s. 2020-2021, mentre per le classi successive, ove ritenuto necessario, l'elenco degli alunni potrà essere reso disponibile nell'area documentale riservata del registro elettronico a cui accedono tutti gli studenti della classe di riferimento.

In caso di comunicazione tramite e-mail, dovrà essere prestata particolare attenzione a inviare la stessa a ciascun destinatario con un messaggio personalizzato oppure a inviarla utilizzando il campo denominato "copia conoscenza nascosta" (ccn) al fine di non divulgare gli indirizzi e-mail forniti dalle famiglie.

Inoltre, si raccomanda di predisporre uno specifico "disclaimer" con cui si evidenzia che i predetti dati personali non possono essere oggetto di comunicazione o diffusione (ad esempio mediante la loro pubblicazione su blog o su social network).

Comunque secondo una prassi ormai consolidata è consentita la pubblicazione al tabellone esposto nella bacheca scolastica dei nominativi degli studenti distinti per classe. In relazione all'avvio del prossimo anno scolastico, al fine di evitare assembramenti e garantire le necessarie misure di sicurezza e distanziamento, il DS predispone una calendarizzazione degli accessi ai tabelloni dell'istituzione scolastica e ne dà preventiva comunicazione alle famiglie degli alunni. Tale modalità di pubblicazione del tabellone in relazione al prossimo anno scolastico dovrebbe essere adottata in via residuale solo qualora l'istituzione scolastica sia sprovvista di registro elettronico o sia impossibilitata ad utilizzare strumenti di comunicazione telematica dei dati.

In tutti i casi gli elenchi relativi alla composizione delle classi, resi disponibili con le modalità sopra indicate, devono contenere i soli nominativi degli alunni e non devono riportare informazioni relative allo stato di salute degli studenti o altri dati personali non pertinenti (es. luogo e data di nascita, ecc.).

Sia in caso di pubblicazione nel registro elettronico sia nel caso di pubblicazione attraverso i tabelloni esposti nella bacheca scolastica, il DS definisce il tempo massimo di pubblicazione che comunque non deve superare i 15 giorni.
VOTI E PUBBLICAZIONE – GIUGNO 2020. Esiti scrutini si pubblicano solo sul registro elettronico. Chiarimenti Ministero. Nuova nota, la 9168 del 9 giugno 2020, del Ministero dell'Istruzione, per ulteriori precisazioni sull'applicazione dell'O.M. n. 11 del 16 maggio 2020 concernente la "valutazione finale degli alunni per l'anno scolastico 2019/2020 e prime disposizioni per il recupero degli apprendimenti". In merito al rapporto tra privacy e voti si è detto tanto e non si dubitava sino alla circolare ministeriale n. 9168 del 9 giugno 2020, che segue ed esplica la nota prot. 8464 del 28 maggio 2020, la quale, per effetto delle deroghe disposte in considerazione della situazione di emergenza sanitaria, ha previsto che, in caso di amissione di alunni alla classe successiva con insufficienze, "anche i voti inferiori a sei decimi sono riportati, oltre che nei documenti di valutazione finale, nei prospetti generali da pubblicare sull'albo on line dell'istituzione scolastica".
Insomma la disposizione ha consentito la pubblicazione anche delle insufficienze sull'albo on line – in luogo della consueta cartellonistica – tra i "prospetti generali", dunque con apparente modalità di estesa pubblicità.
Al di là delle esigenze attuali di evitare affollamenti innanzi ai manifesti cartacei, quanto meno per gli effetti di pubblicità legale il ricorso all'albo della scuola con la tradizionale affissione dei "quadri" poteva comunque considerarsi formalmente superato dalla previsione dell'art. 32, c. 1, la L. 69/2009 per la quale "a far data dal 1 gennaio 2010 (termine poi prorogato al 2011) gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione sui propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati".
Per quanto attiene specificamente la privacy, già nella Newsletter del Garante 12 – 18 giugno 2000 https://www.garanteprivacy.it/home/docweb/-/docweb-display/docweb/46725, si L.: "Continua ad essere diffusa sui mezzi d´informazione l´opinione che l´iniziativa del Ministero della pubblica istruzione di non far rendere note sui quadri esposti al pubblico le valutazioni finali analitiche a carico dei "bocciati" o dei non ammessi all´esame di maturità derivi dalla tutela della riservatezza personale o addirittura dal contenuto della L. n. 675 del 1996.
Ciò non è vero, dal momento che questa L. non prevede nulla del genere.
Certo che la pubblicità degli esiti scolastici è invece la regola in generale: non può infatti dimenticarsi che vi sono essenziali esigenze di controllo sociale e professionale che dipendono proprio dalle conoscibilità delle valutazioni finali.
Successivamente, in un documento del Garante del 28 agosto 2008, a proposito della pubblicità dei voti dell'Esame di Stato si afferma: "Il Garante per la protezione dei dati personali ribadisce che, come già precisato più volte, nessun provvedimento dell´Autorità ha mai impedito la pubblicità dei voti dell´esame di Stato. Il regime attuale relativo alla conoscibilità degli esiti degli esami di maturità è stato stabilito dal Ministero dell´istruzione indipendentemente da ogni parere o richiesta del Garante".
Ed ancora, nel vademecum "La scuola a prova di privacy" del 2016, antecedente all'applicazione del Regolamento UE 679/2016, decorrente dal 25 maggio 2018 a proposito di voti, scrutini, esami di Stato è scritto: "I voti dei compiti in classe e delle interrogazioni, gli esiti degli scrutini o degli esami di Stato sono pubblici. Le

informazioni sul rendimento scolastico sono soggette ad un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell´istruzione. E´ necessario però, nel pubblicare voti degli scrutini e degli esami nei tabelloni, che l´istituto eviti di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle "prove differenziate" sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni, ma deve essere indicato solamente nell´attestazione da rilasciare allo studente".
Dunque è legittima la pubblicazione dei voti in considerazione dei principi di imparzialità e trasparenza della P.A. e del regime di conoscibilità stabilito dal Ministero con i limiti derivanti dalla possibilità di conoscenza di eventuali dati "particolari".
Il D. Lgs. 30 giugno 2003, n. 196, come modificato dal Dlgs. n. 101/2018, per effetto del GDPR, ha preso in considerazione espressamente il trattamento dei dati degli studenti all'art. 96 stabilendo: "1. 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'art. 13 del Regolamento. I dati possono essere successivamente trattati esclusivamente per le predette finalità. 2. Resta ferma la disposizione di cui all'art. 2, c. 2, del decreto del Presidente della Repubblica 24 giugno 1998, n. 249, sulla tutela del diritto dello studente alla riservatezza. Restano altresì ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione nell'albo dell'istituto e di rilascio di diplomi e certificati".
L'art. 1 del Regolamento UE 679/2016 dispone che i dati devono poter circolare liberamente, sebbene in maniera protetta a tutela dei diritti e delle libertà fondamentali delle persone fisiche.
D'altro canto, in attuazione dei principi di imparzialità e trasparenza della PA sono state previste ulteriori forme di accesso volte a operare quel "controllo" escluso dalla L. 241/90. Ci si riferisce in particolare all'accesso civico generalizzato del D. lgs. n. 33/2013, introdotto dal D. lgs. 97/2016 all'art. 5 c. 2 e riconosciuto a chiunque senza formalità "Allo scopo di favorire forme diffuse di controllo sul perseguimento delle funzioni istituzionali e sull'utilizzo delle risorse pubbliche e di promuovere la partecipazione al dibattito pubblico". Pertanto qualunque cittadino "ha diritto di accedere ai dati e ai documenti detenuti dalle pubbliche amministrazioni, ulteriori rispetto a quelli oggetto di pubblicazione" obbligatoria.
Tanto comporta che, in presenza di una istanza di accesso civico generalizzato, nella valutazione del pregiudizio concreto, si faccia riferimento ai principi generali sul trattamento di necessità, proporzionalità, pertinenza e non eccedenza, in conformità al nuovo quadro normativo in materia di protezione dei dati introdotto dal Regolamento (UE) n. 679/2016, verificando se ed in che misura la conoscenza indiscriminata di dati risulti non necessaria o comunque sproporzionata rispetto allo scopo di trasparenza e controllo ed effettuando un "bilanciamento degli interessi" tra

il diritto alla conoscibilità e quello alla protezione dei dati personali (che non significa optare per la parte più pesante ma livellare i due piatti).
In considerazione poi della duplice previsione della «privacy by design» e «privacy by default» dell'art. 25 del GDPR, il titolare del trattamento (nella fattispecie la scuola nella persona del DS) è tenuto a porre in essere «misure tecniche e organizzative adeguate per garantire che siano trattati per impostazione predefinita solo i dati necessari per ogni specifica finalità del trattamento» nonché altre «quali la pseudonimizzazione, volta ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione […]». Esse impongono quindi al titolare di prevedere i rischi che possono incontrare per la tutela dei dati personali, scegliendo di conseguenza quali strumenti adottare.
Ritornando alla nota del 9 giugno essa è stata introdotta dichiaratamente "Al fine di assicurare il rispetto del quadro normativo in materia di protezione dei dati – Regolamento (UE) 2016/679 e d. lgs. 30 giugno 2003, n. 196, come modificato dal d. lgs. n. 101/2018, Codice in materia di protezione dei dati personali". Se ne desume che l'orientamento sia ora cambiato in considerazione del rischio collegato alla circostanza che i voti, una volta esposti, possono rimanere in rete per un tempo indefinito (il che poteva accadere anche prima) e quindi essere "registrati, utilizzati, incrociati" da chiunque con conseguente ingiustificata violazione del diritto alla riservatezza degli studenti.
Precisa la nota "che per pubblicazione on line degli esiti degli scrutini delle classi intermedie delle scuole primarie, secondarie di primo grado e secondarie di secondo grado *si intende la pubblicazione in via esclusiva nel registro elettronico*", ribadendo quindi quanto già prescritto nella disposizione di maggio.
Ma in merito alle modalità di pubblicazione è ulteriormente chiarito che "gli esiti degli scrutini con la sola indicazione per ciascun studente "ammesso" e "non ammesso" alla classe successiva, sono pubblicati, distintamente per ogni classe, nell'area documentale riservata del registro elettronico, cui accedono tutti gli studenti della classe di riferimento. Diversamente i voti in decimi, compresi quelli inferiori a sei decimi, riferiti alle singole discipline, 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".
Dunque si evince che la classe potrà L.re soltanto il giudizio di ammissione o non ammissione mentre l'accesso ai propri voti resta limitato a ciascuno studente con proprie credenziali.
La stessa nota raccomanda i dirigenti di predisporre uno specifico "disclaimer" con esclusione di responsabilità in caso di divulgazione del dato. A tal proposito è singolare come invece la normativa in tema di accesso civico preveda in generale la riutilizzabilità del dato (artt. 7 e 7 bis)
La pubblicazione all'albo cartaceo è consentita in via del tutto eccezionale e residuale nei casi di mancanza di registro elettronico "con la sola indicazione di ammissione/non ammissione alla classe successiva". Infine, fermo il rispetto dei noti principi di riservatezza, per evitare gli assembramenti in tal caso è prevista una calendarizzazione degli accessi ed un tempo massimo di pubblicazione non eccedente i 15 giorni.

Ebbene non si tratta di una norma derogatoria in considerazione di circostanze eccezionali ma di un cambiamento di orientamento dinanzi ad un impianto normativo allo stato invariato o comunque non significativamente modificato.
Che ne è della trasparenza (e imparzialità) della valutazione che continua ad essere richiamata nell'art. 1 del DPR 122/08 e del Dlgs 62/2017?
Considerati i principi alla base del diritto di accesso di cui al D. lgs. 33/13 come modificato dal D. lgs. 97/2016 non potrebbe accadere che le scuole si vedano destinatarie di numerose istanze di accesso (civico) al fine di realizzare quel controllo sull'operato in presenza di insufficienze?
Pubblicità degli scrutini. La normativa in materia di protezione dei dati, sia europea, con il Regolamento (UE) 2016/679, che nazionale, con il d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. n. 101/2018, recante il "Codice in materia di protezione dei dati personali", a integrazione di quanto indicato nella citata nota n. 8464/2020, prevede adempimenti piuttosto stringenti a tutela dei dati personali degli alunni. Gli scrutini delle classi intermedie delle scuole primarie, secondarie di primo grado e secondarie di secondo grado possono essere pubblicati solamente sul registro elettronico. Gli esiti degli scrutini con la l'indicazione per ciascun studente "ammesso" e "non ammesso" alla classe successiva, sono pubblicati, per ogni classe, nell'area bacheca riservata del registro elettronico, cui possono accedere solamente gli studenti della classe di riferimento.
Ancora più stringente la visione dei voti relativi agli insegnamenti e alle educazioni, per ogni ordine e grado dell'istruzione pubblica. La nota, nel sottolineare la valutazione in decimi, e la possibilità, eccezione prevista solo per questo anno scolastico, di una valutazione con voti inferiori a sei decimi, riferiti alle singole discipline, dispone che i voti siano riportati sia nel documento di valutazione, che nell'area riservata del registro elettronico in uso in ciascuna istituzione scolastica.
Nel caso di specie l'accesso alla visione deve essere garantito e limitato esclusivamente, e con le proprie credenziali personali, all'alunno o al genitore, se minorenne. Il ministero interviene, a proposito, anche sull'invalsa cattiva abitudine, di studenti ma anche dei genitori, di pubblicare i voti, attraverso fotografie o screen shot, su blog o su social network. A tal riguardo la scuola deve trasformarsi in fonte di cognizione e prevedere la predisposizione di alcuni spazi attraverso i quali educere i titolari del diritto alla visione del voto, di questa tipologia di limitazione.
L'albo della scuola
Il ricorso all'albo della scuola con la classica ma ormai tramontata affissione dei risultati è consentito esclusivamente alle istituzioni *prive assolutamente di registro elettronico*. In questo caso si possono pubblicare solo gli esiti degli scrutini, con l'indicazione di ammissione/non ammissione alla classe successiva. Essendo ancora in un momento post-pandemico, (fase 2-3) con enormi restrizioni, il DS predisporrà una calendarizzazione, non superiore a 15 giorni, per contingentare l'accesso all'albo dell'istituzione scolastica di genitori o alunni.
Esiti degli scrutini di ammissione agli esami di maturità
Stesse modalità sono previste dalla nota per la pubblicizzazione degli esiti degli scrutini e dei crediti scolastici attribuiti ai candidati in procinto di sostenere l'esame di maturità. Per gli esiti degli scrutini bisogna riportare la sola indicazione "ammesso" e "non ammesso" alla prova d'esame; per i crediti scolastici attribuiti ai

candidati, ciascun alunno sarà posto nelle condizioni di accedere ad un'area riservata del registro elettronico per classe di appartenenza.
I voti riferiti alle singole discipline sono riportati, come già detto per tutti gli altri ordini e tutte le altre circostanze, nel documento di valutazione e nell'area riservata del registro elettronico. È consentita la pubblicazione all'albo della scuola solo degli esiti degli scrutini di ammissione agli esami di Stato e dei crediti scolastici attribuiti ai candidati, nel caso in cui l'istituzione non disponga di registro elettronico. La pubblicazione non deve superare 30 giorni e deve prevedere un accesso contingentato all'albo.
OPEN DATA E RIUTILIZZO DEI DATI. I dati pubblicati on line non sono liberamente utilizzabili da chiunque per qualunque finalità. L'obbligo previsto dalla normativa in materia di trasparenza on line della PA di pubblicare dati in "formato aperto", non comporta che tali dati siano anche "dati aperti", cioè liberamente utilizzabili da chiunque per qualunque scopo. Il riutilizzo dei dati personali non deve pregiudicare, anche sulla scorta della direttiva europea in materia, il diritto alla privacy.
Le PA dovranno quindi inserire nella sezione denominata "Amministrazione trasparente" sui propri siti web un alert con cui si informa il pubblico che i dati personali sono riutilizzabili in termini compatibili con gli scopi per i quali sono raccolti e nel rispetto del norme sulla protezione dei dati personali. I dati sensibili e giudiziari non possono essere riutilizzati.
DURATA DEGLI OBBLIGHI DI PUBBLICAZIONE. Il periodo di mantenimento on line dei dati è stato generalmente fissato in 5 anni dal D. Lgs.. Sono previste però alcune deroghe, come nell'ipotesi in cui gli atti producano i loro effetti oltre questa scadenza. In ogni caso, quando sono stati raggiunti gli scopi per i quali essi sono stati resi pubblici e gli atti hanno prodotto i loro effetti, i dati personali devono essere oscurati anche prima del termine dei 5 anni.
MOTORI DI RICERCA. L'obbligo di indicizzare i dati nei motori di ricerca generalisti (es. Google) durante il periodo di pubblicazione obbligatoria è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza. Vanno dunque esclusi gli altri dati che si ha l'obbligo di pubblicare per altre finalità di pubblicità (es. pubblicità legale sull'albo pretorio, pubblicazioni matrimoniali ecc). Non possono essere indicizzati (e quindi reperibili attraverso i motori di ricerca) i dati sensibili e giudiziari.
IL REGOLAMENTO UE/2016/679 E LA SCUOLA. Nella scuola sarà necessario acquisire l'autorizzazione al trattamento? È possibile l'esercizio del diritto all'oblio? Il D. Lgs. 101/2018 conferma la liceità del trattamento per l'esecuzione di un compito di interesse pubblico connesso all'esercizio di pubblici poteri di cui è investito il titolare e non prevede per questi casi né il consenso né la possibilità che l'interessato possa chiederne la cancellazione (cosiddetto "diritto all'oblio"), se non quando i dati non siano più necessari rispetto alle finalità per le quali sono stati trattati.
L'art. 2-sexies, c. 2, lettera bb) definisce di interesse pubblico rilevante il trattamento dei dati relativi al servizio di istruzione, autorizzando di fatto il trattamento dei dati personali nelle scuole che pertanto dispongono della base giuridica necessaria a supportare il trattamento dei dati effettuati.
Nella scuola è autorizzato anche il trattamento dei dati sensibili? Il regolamento europeo sottolinea la necessità di una specifica protezione per dati personali

considerati “sensibili”, ribadendo che tali dati non dovrebbero essere oggetto di trattamento, a meno che il trattamento non sia consentito da norme specifiche degli stati membri, per compiti di interesse pubblico o per l’esercizio di pubblici poteri di cui è investito il titolare del trattamento. Il D.M. 305/2006 con cui il MIUR autorizza il trattamento dei dati sensibili da parte delle scuole individuandone ambiti e finalità e gli specifici Provvedimenti del Garante su particolari trattamenti non previsti nel DM consentono alle scuole di continuare a trattare dati sensibili.

Viene introdotto il principio di “responsabilizzazione” in base al quale il bilanciamento fra legittimo interesse del titolare o del terzo e diritti e libertà dell’interessato non spetta all’Autorità ma è compito dello stesso titolare. Si conferma che l’interesse legittimo del titolare o del terzo deve prevalere sui diritti e le libertà fondamentali dell’interessato per costituire un valido fondamento di liceità.

E’ necessario modificare i contenuti dell’informativa che le istituzioni scolastiche sono tenute a fornire agli interessati? Il regolamento europeo conferma il diritto dell’interessato a ricevere informazioni relative all’identità del titolare e del responsabile del trattamento dei dati che lo riguardano, alle finalità per cui sono raccolti, ai diritti degli interessati. Nessuna significativa modifica si prevede pertanto rispetto ai contenuti delle informative già fornite dalle scuole, se non relativamente alla necessità che, accanto all’identità di titolare e responsabile, sia indicato anche un dato di contatto.

Il regolamento indica in modo tassativo i contenuti dell’informativa che sono più ampi rispetto al Codice. Il titolare deve sempre specificare:

- Identità e dati di contatto del titolare del trattamento
- Identità e dati di contatto del RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer), ove esistente
- Finalità del trattamento e la base giuridica del trattamento
- Periodo di conservazione dei dati o i criteri seguiti per stabilire tale periodo di conservazione
- Diritto di presentare un reclamo all’autorità di controllo.
- Esistenza di processi decisionali automatizzati(compresa la profilazione)

Il GDPR conferma che il titolare del trattamento è il soggetto sul quale ricadono le maggiori responsabilità della gestione dei dati ed in particolare quella di organizzare, monitorare e migliorare continuamente un sistema di protezione dei dati personali trattati, con attenzione specifica a quelli sensibili e giudiziari, e di nominare un responsabile del trattamento.

Si ritiene possa essere confermata la titolarità del trattamento in capo al DS e l’individuazione del DGSA quale responsabile del trattamento. Nessun riferimento è presente nel Regolamento in merito alla figura dell’incaricato del trattamento che riteniamo potrebbe essere assorbita dalla figura del sub-responsabile introdotta dal Regolamento. Il Regolamento fissa più dettagliatamente rispetto al Codice le caratteristiche dell’atto con cui il titolare designa un responsabile del trattamento attribuendogli specifici compiti: deve trattarsi, infatti, di un contratto (o altro atto giuridico conforme al diritto nazionale) che deve dimostrare che il responsabile fornisce “garanzie sufficienti” a mettere in atto le misure tecniche e organizzative adeguate a consentire il rispetto delle istruzioni impartite dal titolare e, in via generale, delle disposizioni contenute nel regolamento.

Il Regolamento consente la nomina di sub-responsabili del trattamento da parte di un responsabile per specifiche attività di trattamento, nel rispetto degli stessi obblighi contrattuali che legano titolare e responsabile primario. Il responsabile primario risponde dinanzi al titolare dell'inadempimento dell'eventuale sub-responsabile, anche ai fini del risarcimento di eventuali danni causati dal trattamento, salvo dimostri che l'evento dannoso non gli sia in alcun modo imputabile (inversione onere della prova).
Nel corso di un'informativa alle OO.SS. del 2 agosto 2018, il MIUR ha illustrato un modello di Registro unico delle attività di trattamento per le istituzioni scolastiche. Il Registro delle attività di trattamento che deve contenere le seguenti informazioni :

- Nome e contatto del titolare e del responsabile della protezione dei dati
- Finalità del trattamento
- Descrizione categorie interessati
- Categorie destinatari termini previsti per l'eventuale cancellazione
- Descrizione sintetica misure di sicurezza tecniche e organizzative adottate

Il registro deve essere a disposizione delle autorità di controllo.
Il Regolamento prevede altresì che ogni responsabile del trattamento tenga un registro delle attività di trattamento che deve contenere le seguenti informazioni:

- Nome e contatto del responsabile o dei responsabili, del titolare, del responsabile della protezione dei dati
- Descrizione sintetica misure di sicurezza tecniche e organizzative adottate

Il Registro deve essere a disposizione delle autorità di controllo.
Nelle indicazioni date alle istituzioni scolastiche con la nota n. 563 del 22 maggio 2018 il MIUR ha sostenuto che "ciascun istituto scolastico, in virtù della propria autonomia, deve dotarsi in via prioritaria del Responsabile della protezione dati personali". Come indicato dall'art. 37, c. 3, del Regolamento, la nota MIUR prevede che è consentito a più scuole di avvalersi di un unico Responsabile e che gli Uffici Scolastici Regionali "dovranno svolgere un fondamentale ruolo di interlocuzione e di coordinamento nei confronti delle istituzioni scolastiche per promuovere soluzioni condivise".
Nella scuola è necessario che il titolare del trattamento effettui la valutazione di impatto preliminarmente al trattamento dei dati? La valutazione di impatto è una valutazione sistematica dei possibili rischi che presenta un particolare trattamento sulla protezione dei dati. Le tipologie di trattamento soggette alla valutazione di impatto devono essere definite in un pubblico elenco da un'autorità di controllo indipendente. Si ritiene che su tutti i trattamenti delle istituzioni scolastiche eventualmente individuati a rischio debba essere l'amministrazione scolastica ad effettuare la valutazione di impatto.
Diritto di accesso. Il diritto di accesso prevede anche il diritto di ricevere (gratuitamente) una copia dei dati personali oggetto di trattamento. Se la richiesta avviene attraverso mezzi elettronici, salvo diversa indicazione dell'interessato, le informazioni sono fornite in formato elettronico di uso comune.
Diritto alla cancellazione (diritto all'oblio). Il diritto cosiddetto "all'oblio" si configura come il rafforzamento del diritto alla cancellazione dei propri dati personali ed ha un campo di applicazione più esteso di quello previsto dal Codice. Il titolare è obbligato alla cancellazione, tra l'altro, anche quando i dati personali non sono più necessari rispetto alle finalità per le quali sono stati raccolti. Si prevede l'obbligo per i titolari di

informare della richiesta di cancellazione altri titolari che trattano i dati personali cancellati, compresi "qualsiasi link, copia o riproduzione".
Diritto alla "portabilità" dei dati. Si tratta di uno dei nuovi diritti presenti nel Regolamento (già utilizzato per il numero telefonico) riferito esclusivamente ai trattamenti automatizzati (quindi non si applica agli archivi o registri cartacei). Consiste nel diritto dell'interessato di ricevere dal titolare del trattamento in un formato strutturato, di uso comune e leggibile da dispositivo automatico, i dati personali che lo riguardano e di trasmetterli ad altro titolare senza impedimenti da parte del titolare precedente. Se possibile tecnicamente, l'interessato ha diritto alla trasmissione diretta da un titolare all'altro.
Con la nota 563 del 22 maggio 2018 in materia di "Regolamento generale sulla protezione dei dati UE/2016/679 - Responsabile della protezione dei dati personali", il Miur ha fornito indicazioni alle scuole. Cosa deve fare una scuola?

- identificare i trattamenti e predisporre il Registro dei trattamenti;
- definire i ruoli;
- nominare il RPD-DPO (Responsabile della protezione dei dati - Data Protection Officer;
- analizzare il rischio;
- organizzare ed implementare le misure di sicurezza;
- predisporre la documentazione.
- valutazione di impatto
- formalizzazione dei processi
- informative agli interessati
- manifestazioni di consenso degli interessati.

Data breach. Prima non era stabilito alcun obbligo di notifica delle eventuali violazioni dei dati personali. Adesso, con la nuova normativa, è stato sancito l'obbligo, per il titolare, di comunicare le violazioni ("Data breach") all'Autorità Garante, possibilmente entro 72 ore dalla scoperta, nonché al soggetto interessato.
Fasi della procedura in caso di furto di PC e rischio di data breach:

- denuncia alle Forze dell'ordine;
- avvertire anche l'ente locale di riferimento,
- per il data breach, entro 48 ore, protocollare la mail al DPO/Amministratore di sistema;
- eventuale comunicazione al Garante della privacy.

Responsabile della Protezione dei dati personali – DPO. Prima non era prevista alcuna figura di raccordo tra i soggetti del trattamento e l'Autorità Garante. Adesso è prevista l'introduzione della figura del Data Protection Officer (DPO), figura professionale obbligatoria che dovrà avere requisiti e competenze elevate. Il DPO potrà essere un collaboratore esterno. E' convinzione diffusa, e pericolosa, che il DPO - Responsabile della Protezione dei dati personali sia qualcuno che debba svolgere delle attività per conto del Titolare (disporre modulistica, formazione, ecc). Il GDPR, invece, affida al DPO il compito opposto, ossia di "sorvegliare" che il Titolare svolga o faccia svolgere da qualcuno quelle attività (art.37). L'unica attività che il DPO è chiamato a svolgere su richiesta del Titolare è la "consulenza". Per il resto il DPO deve essere un "occhio" del Garante, con cui è obbligato a cooperare (art.37 c.1 d). Per il resto deve essere del tutto autonomo nello svolgimento della sua attività di controllo, senza alcun condizionamento (art.38 c.3).

Ciascun istituto scolastico deve quindi dotarsi in via prioritaria del Responsabile della protezione dei dati personali. Tale figura, interna o esterna, deve essere connotata dei requisiti di autonomia e indipendenza, operare senza conflitto di interessi e possedere specifiche competenze in materia di trattamento di dati personali. E' consentito a più scuole di avvalersi di un unico responsabile. Le scuole devono assicurare, inoltre, una formazione adeguata e capillare sui nuovi temi e le nuove problematiche.
Requisiti e corso di formazione di nove ore per il Responsabile della protezione dei dati personali (DPO), nota Miur 563/2018. Requisiti:
autonomia e indipendenza, senza conflitto di interessi;
specifiche competenze in materia di trattamento dei dati personali.
Il MIUR provvederà a rendere accessibile a tutto il personale scolastico il corso di formazione on line, della durata di nove ore. Verrà, poi, definita l'organizzazione di un sistema di formazione a rete, prevedendo degli incontri formativi interregionali indirizzati in via prioritaria ai DS e ai DSGA.
Per la nomina del DPO di solito i costi si aggirano intorno ai 700-800€ iva esclusa. Se poi si occupa anche di altre questioni relative agli espletamenti AGID, il costo si aggira intorno ai 1500 €.
Registro delle attività di trattamento dei dati personali. Il Miur fornisce un modello standard di Registro delle attività di trattamento dei dati personali. Il Miur mette a disposizione delle scuole i seguenti strumenti:

- Registro delle attività di trattamento dei dati personali vuoto;
- Registro delle attività di trattamento dei dati personali compilato;
- Guida alla compilazione del registro delle attività di trattamento dei dati personali.

Il Registro dei trattamenti proposto dal Miur prevede le seguenti sezioni:
trasferimenti all'estero: indicare la condizione che autorizza il trasferimento dei dati in Stati al di fuori dell'Unione Europea o ad organizzazioni internazionali. Di solito questa sezione non riguarda le scuole;
misure di sicurezza: controllo accessi fisici e informatici, codifica di procedure, cifratura dei dati, report e log, backup;
contitolari del trattamento: il Miur nel caso di assunzione del personale sia a tempo determinato che indeterminato;
responsabile esterno del trattamento: persona fisica o giuridica che tratta dati personali per conto del titolare: esempio il Miur in caso di utilizzo del Sidi, il fornitore locale di servizi, ecc.
Indicazioni sul trattamento dei dati. I dati trattati dalla scuola devono rispondere ai criteri della liceità, della non eccedenza rispetto alla finalità dell'atto specifico o istituzionale, del consenso e dell'informativa. Le suddette regole sono state confermate dal GDPR (679/16) e ovviamente dal decreto attuativo D. Lgs. 101/18. L'unica novità consiste nel maggior coinvolgimento del minorenne. I riferimenti sono l'art. 8 del Nuovo regolamento europeo e l'art. 2- quinquies del Decreto attuativo. Quest'ultimo ha italianizzato l'età minima per esercitare il consenso e il diritto all'informativa, portandola da sedici anni (GDPR) ai quattordici anni. L'indicazione, ovviamente vale anche nei casi di autonoma gestione di alcuni dati personali (foto e video) e di azioni verso l'autorità giudiziaria in previsione dell'ammonimento (L. 71/17 "Disposizioni per la prevenzione e il contrasto al cyberbullismo).

E’ invece assente la spinosa tematica della liceità della pubblicazione di foto e video sul sito o pagina social afferenti la scuola. Sarebbe stato sufficiente confermare quanto già espresso nel documento “Scuola a prova di privacy” (novembre 2016): “Le istituzioni scolastiche pubbliche possono trattare solamente i dati personali necessari al perseguimento di specifiche finalità istituzionali oppure quelli espressamente previsti dalla normativa di settore. Per tali trattamenti, non sono tenute a chiedere il consenso degli studenti.” Il suddetto passaggio si basava sull’art. 18 del D. Lgs. 196/03 (Vecchio Codice Privacy) che recitava al c. 2 e 4 “Qualunque trattamento di dati personali da parte di soggetti pubblici è consentito soltanto per lo svolgimento delle funzioni istituzionali. Salvo quanto previsto nella Parte II per gli esercenti le professioni sanitarie e gli organismi sanitari pubblici, i soggetti pubblici non devono richiedere il consenso dell’interessato.” Il tempo imperfetto che caratterizza il verbo basava è giustificato dal fatto che il D. Lgs. 101/18 ha abrogato l’art. 18 del disposto 196/03. L’unico riferimento esplicito è l’art. 2 (Nuovo codice Privacy) che però fa riferimento alla comunicazione fra titolari che effettuano trattamenti di dati personali “ammessa quando è comunque necessaria per lo svolgimento di compiti di interesse pubblico“

Concludendo il quadro si presenta poco chiaro, dando la possibilità a chi ha sempre sostenuto la tesi del divieto di pubblicazione di tornare alla carica, dimostrando la fondatezza del principio che se non esplicitamente previsto dalla normativa, allora non si pubblica nulla.

CASI DI PRIVACY A SCUOLA, LE FAQ DEL GARANTE - DICEMBRE 2019. Il Garante della privacy ha pubblicato una breve guida dove tratta alcune casistiche in materia di privacy e scuola.

Temi in classe. Non lede la privacy l'insegnante che assegna ai propri alunni lo svolgimento di temi riguardanti il loro mondo personale. Qualora gli elaborati degli studenti, vengano letti in classe, è l'insegnante che deve trovare l'equilibrio. Restano comunque validi gli obblighi di riservatezza già previsti per il corpo docente riguardo il segreto d’ufficio e professionale, nonché quelli riguardanti la tutela dei dati personali contenuti nei temi degli studenti.

Soggetti esterni e immagini. Nella scuola sono diverse le occasioni che possono portare alla comunicazione e alla diffusione dell’immagine di un minore. Il primo caso è quello di operatori esterni, fotografi, che riprendono il minore al fine di documentare un certo evento (l’inizio dell’anno scolastico, la recita, la manifestazione sportiva ecc.). In questo caso il comportamento che la scuola deve tenere deve essere improntato alla massima vigilanza sulle attività che si svolgono al suo interno. Relativamente al caso concreto il dirigente deve verificare le credenziali del fotografo e fare in modo di mettere lo stesso in contatto con le famiglie. Saranno le stesse a decidere se prestare il loro consenso alla realizzazione fotografica. In questo caso il consenso è necessario, trattandosi di soggetto privato.

La stessa procedura va adottata nel caso in cui la scuola, nel corso di un partenariato con soggetti esterni, gestisca eventi o manifestazioni, le cui rappresentazioni fotografiche verranno usate per comunicare l’evento a mezzo stampa o televisione. La scuola può esclusivamente mettere in contatto il soggetto esterno con le famiglie per la gestione della procedura di richiesta del consenso. Pensiamo ad un percorso teatrale che prevede la ripresa finale, che il soggetto

partner vorrebbe utilizzare a fini divulgativi. La scuola deve fare in modo che le famiglie vengano informate sull'uso che si vuole fare della ripresa e in quel contesto, se d'accordo, può esprimere il consenso al trattamento delle immagini.
La scuola, al contrario, potrebbe organizzare essa stessa la realizzazione di un servizio fotografico mirato a documentare un certo evento. L'attività è lecita se esercitata nell'ambito di attività istituzionali, ma, per quanto riguarda la diffusione di tali immagini, non si rinviene una disposizione che lo consenta. Le immagini devono rimanere agli atti della scuola, in qualità di documentazione del percorso didattico e/o formativo.
Gli stessi principi valgono per i filmati aventi come soggetto i bambini. Al fine della realizzazione o documentazione di attività istituzionali, la scuola deve provvedere alla loro conservazione documentale. Se, invece, la scuola intende utilizzare i filmati per la partecipazione a mostre, fiere, concorsi, occorre fare in modo che il soggetto titolare del trattamento (ad es. Rai, tv locale, associazioni, ecc.) ottenga dall'interessato il consenso. La scuola farà da tramite tra il titolare e la famiglia.
Affrontiamo il caso più delicato relativo alla riproduzione di immagini di minori su giornalini di scuola e/o su siti web di libero accesso.
Il giornale di classe o di scuola rientra nella consuetudine della didattica di ogni ordine e grado. Le cautele da adottare dipendono dal grado di diffusione del giornalino stesso. Una distribuzione limitata alle famiglie degli allievi va gestita come comunicazione di dati personali. Pertanto, il genitore, all'inizio dell'anno scolastico, in occasione della consegna dell'informativa, ex art. 13 del Codice, avrà notizia dell'uso che sarà fatto delle immagini e, se lo riterrà opportuno, chiederà, ai sensi dell'art. 7 del Codice, che le immagini non vengano utilizzate.
Se, diversamente, il giornalino ha una diffusione indiscriminata, ad esempio viene distribuito sul territorio, non v'è dubbio che si tratti di diffusione di dati personali. In questo caso non è consentito pubblicare foto di minori riconoscibili, anche se legate ad eventi positivi. La ragione di tale comportamento da tenere sta nell'analisi degli indicatori di liceità che devono condurre l'azione. Gli indicatori della pertinenza e non eccedenza sono in primo piano. Essi comportano una scrupolosa verifica dell'adeguatezza dei dati agli scopi del trattamento. Se scopo del trattamento specifico è il riconoscimento di un merito al minore per un suo successo scolastico, non v'è ragione di divulgare una sua foto corredata da nome e cognome, poiché basterebbe citare il suo nome di battesimo e la classe per evidenziarne i meriti.
Caso ancora più potenzialmente pericoloso è il sito web della scuola e la pubblicazione sullo stesso del giornalino scolastico. La messa a disposizione della rete, senza alcuna limitazione dell'accesso, crea rischi potenziali di utilizzo delle informazioni illimitati. Ma, senza considerare questo estremo effetto dell'uso delle immagini, basta soffermarsi sul concetto di necessarietà del trattamento del dato. Gli stessi risultati vanno perseguiti con il mezzo e le modalità meno invasive.
Servizio mensa. E' illecito pubblicare sul sito della scuola il nome e cognome degli studenti i cui genitori sono in ritardo nel pagamento della retta o del servizio mensa. Lo stesso vale per gli studenti che usufruiscono gratuitamente del servizio mensa in quanto appartenenti a famiglie con reddito minimo. Gli avvisi devono avere carattere generale, mentre le comunicazioni indirizzate alle singole persone, devono essere a carattere individuale.

Comunicazione di dati personali a soggetti privati. Il Garante si è occupato anche della comunicazione e diffusione alle aziende private e alle P.A. dei dati personali degli studenti: questo è ammesso al solo fine di agevolare il loro inserimento professionale, l'orientamento, la formazione. Al fine di agevolare l'orientamento, la formazione e l'inserimento professionale le scuole, su richiesta degli studenti, possono comunicare e diffondere alle aziende private e alle pubbliche amministrazioni i dati personali dei ragazzi.
Rapporti con le organizzazioni sindacali (Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico - Deliberazione n. 23 del 14 giugno 2007). Le pubbliche amministrazioni possono comunicare a terzi in forma realmente anonima dati ricavati dalle informazioni relative a singoli o a gruppi di lavoratori: si pensi al numero complessivo di ore di lavoro straordinario prestate o di ore non lavorate nelle varie articolazioni organizzative, agli importi di trattamenti stipendiali o accessori individuati per fasce o qualifiche/livelli professionali, anche nell'ambito di singole funzioni o unità organizzative. Sulla base delle disposizioni dei contratti collettivi, i criteri generali e le modalità inerenti a determinati profili in materia di gestione del rapporto di lavoro sono oggetto di specifici diritti di informazione sindacale preventiva o successiva.
Resta disponibile per l'organizzazione sindacale anche la possibilità di presentare istanze di accesso a dati personali attinenti ad uno o più lavoratori su delega o procura (art. 9, c. 2, del Codice), come pure la facoltà di esercitare il diritto d'accesso a documenti amministrativi in materia di gestione del personale, nel rispetto delle condizioni, dei limiti e delle modalità previsti dalle norme vigenti e per salvaguardare un interesse giuridicamente rilevante di cui sia portatore il medesimo sindacato (artt. 59 e 60 del Codice). Il rifiuto, anche tacito, dell'accesso ai documenti amministrativi, è impugnabile presso il tribunale amministrativo regionale, la Commissione per l'accesso presso la Presidenza del Consiglio dei ministri o il difensore civico (artt. 25 e ss. l. 7 agosto 1990, n. 241; art. 6 d.P.R. 12 aprile 2006, n. 184). L'amministrazione può anche rendere note alle organizzazioni sindacali informazioni personali relative alle ritenute effettuate a carico dei relativi iscritti, in conformità alle pertinenti disposizioni del contratto applicabile e alle misure di sicurezza previste dal Codice (artt. 31-35).
Compensi. Risulta proporzionato indicare il compenso complessivo percepito dai singoli dipendenti (determinato tenendo conto di tutte le componenti, anche variabili, della retribuzione). Non è però giustificato riprodurre sul web le dichiarazioni fiscali o la versione integrale dei cedolini degli stipendi.
FORMAZIONE SULLA PRIVACY. In considerazione delle diverse sentenze sulla formazione sicurezza, si può andare per estensione: tutta la formazione può rientrare nelle 40 ore + 40 ore, senza distinzione tra c. a e b dell'art. 29 attività funzionali. In genere sulle ore dedicate ai Collegi e ai Dipartimenti avanza qualcosa. Se si riesce a deliberare in Collegio un piano di formazione con delle ore, quelle diventano obbligatorie. Il recupero lo si può fare anche calcolando le volte che i docenti si assentano (tranne malattia) ai Collegi e ai Consigli di classe. E' opportuno che dopo la delibera del Collegio, il Piano di formazione venga inserito in contrattazione d'Istituto.

LA PRIVACY E IL DIRITTO DI ACCESSO ALLA DOCUMENTAZIONE AMMINISTRATIVA. La trasparenza e la pubblicità sono principi generali dell'attività amministrativa sanciti dalla stessa Carta Costituzionale e presenti nella L. 241/90 che riconosce ai cittadini il diritto di visionare ed estrarre copia di documenti prodotti e detenuti dall'Amministrazione per la tutela di situazioni giuridicamente rilevanti. L'art. 22 della L. 241/90 definisce tale diritto come diritto di accesso e chiama interessati tutti i soggetti privati, compresi quelli portatori di interessi pubblici e diffusi, che abbiano un interesse diretto, concreto e attuale, corrispondente ad una situazione giuridicamente tutelata e collegata al documento al quale è chiesto l'accesso. Tale interesse è però spesso in contrasto con quello di altri soggetti, che la L. chiama controinteressati, i quali dall'esercizio dell'accesso potrebbero vedere compromesso il loro diritto alla riservatezza. Esiste perciò un possibile conflitto tra diritto di accesso e tutela dei dati personali che richiede la necessità di bilanciare questi due interessi contrapposti. Gli orientamenti giurisprudenziali sembrano privilegiare il diritto di accesso, ritenendolo preponderante rispetto al diritto alla riservatezza, fatta salva la necessità di tutela e protezione di dati sensibili la cui conoscenza non risulti indispensabile alla tutela degli interessi del soggetto che ha richiesto l'accesso. Nella giurisprudenza amministrativa sono perciò molto frequenti le soluzioni di "buon senso" che riconoscono il diritto di accesso con particolari accorgimenti che non rendano visibili le parti di un documento contenenti i dati da tutelare, al fine di bilanciare il soddisfacimento di entrambi gli interessi.

I casi più comuni in cui l'amministrazione scolastica deve consentire l'accesso senza eccezioni sono i seguenti:

- elaborati scritti e atti della commissione giudicatrice in favore dei candidati a pubblici concorsi
- compiti scritti
- documenti relativi a scrutini intermedi e finali
- verbali interrogazioni orali e verbali consigli di classe alunni ai genitori di alunni non promossi per le sole parti che riguardano l'alunno e omissione dati altri alunni
- atti dei procedimenti di trasferimento, utilizzazione a personale che abbia prodotto ricorso avverso mancato trasferimento o utilizzazione
- atti del fascicolo personale dei richiedenti
- atti e relazione ispettiva di personale sottoposto a ispezione o procedimento disciplinare
- atti e documenti relativi all' esame di stato
- documentazione scolastica di alunni da parte del genitore separato/divorziato non affidatario.

Il D.M. n. 60/1996 autorizza l'amministrazione scolastica al diniego di accesso per le seguenti categorie di documenti:

- rapporti informativi sul personale
- informazioni di carattere psico-attitudinale
- accertamenti e dichiarazioni medico-legali
- documenti relativi alla salute
- atti dell'autorità giudiziaria o della procura della corte dei conti da cui si delinei una responsabilità civile, penale o amministrativa.

Lo stesso D.M. n. 60/1996 autorizza l'amministrazione scolastica al differimento dell'accesso per le seguenti categorie di documenti:

- relazione finale in caso di incarichi ispettivi a dipendenti, scuole vigilate
- elaborati e schede di valutazione di concorsi e selezioni di personale
- offerte contrattuali nei procedimenti di scelta del contraente.

A partire dalla L. 241/1990, la trasparenza è stata elevata al rango di imperativo categorico. È proprio in contrapposizione al diritto di accesso che si pone il problema della tutela della riservatezza dei soggetti coinvolti. Diritto di accesso e diritto alla privacy sono due estremi antitetici che necessitano di essere bilanciati. Il legislatore ha risolto questo problema codificando una serie di principi-guida, contenuti sia nella L. sul procedimento che nel Codice sulla privacy → trovare, nei casi concreti, un punto di equilibrio tra accesso e riservatezza → sistema di bilanciamento: graduazione del diritto di accesso in relazione alla tipologia di dati personali.

L'art. 24 della L. del 1990 afferma in via generale la prevalenza del diritto di accesso in tutte le ipotesi in cui questo è preordinato all'esercizio del diritto di difesa di un interesse giuridicamente rilevante, per curare o per difendere i propri interessi giuridici. Nel caso di documenti contenenti dati sensibili o giudiziari, l'accesso è consentito nei limiti in cui sia strettamente indispensabile, mentre in presenza di dati idonei a rivelare lo stato di salute e la vita sessuale (dati ultra-sensibili o sensibilissimi) l'accesso è consentito nei termini previsti dall'art. 60 D. Lgs. 196/2003.

In sintesi, è possibile delineare un sistema di tutela dei dati personali contenuti in documenti amministrativi, ai quali si chiede l'accesso, basato su tre livelli di protezione:

il primo livello, quello più alto, riguarda i cd. dati ultra-sensibili (stato di salute, vita sessuale), per i quali l'accesso è consentito solo se la situazione giuridicamente rilevante che si intende tutelare con la richiesta di accesso è di rango almeno pari ai diritti dell'interessato, ovvero consiste in un diritto della personalità o in un altro diritto o libertà fondamentale e inviolabile;

ad un secondo livello di protezione si pongono i cd. dati sensibili (origine razziale ed etnica, convinzioni religiose, filosofiche o opinioni politiche) e i dati giudiziari, accessibili nei limiti in cui sia strettamente indispensabile per la tutela dei propri interessi;

infine, meno intensa è la protezione dei cd. dati comuni, ai quali è possibile accedere quando la loro conoscenza è necessaria per curare o per difendere gli interessi giuridici dell'istante.

Per i dati sullo stato di salute e sulla vita sessuale delle persone, il destinatario della richiesta dell'accesso, per decidere se accogliere, anche solo in parte, l'istanza, deve verificare se il diritto che si intende far valere o difendere, sia almeno "di pari rango" rispetto al diritto da preservare → solo se il diritto del richiedente rientra nella categoria dei diritti della personalità o è compreso tra altri diritti fondamentali ed inviolabili.

Il raffronto tra la situazione giuridicamente rilevante e la tutela della riservatezza dei dati ultra-sensibili deve essere empirico; la valutazione in concreto dei diversi diritti soggettivi è finalizzata, infatti, ad evitare il rischio di soluzioni precostituite basate su una scala gerarchica astratta dei diritti in contesa.

Come conciliare dunque privacy e disciplina del diritto d'accesso agli atti amministrativi (L. 241/1990) e principio di trasparenza? D. Lgs. 14-3-2013, n. 33, cd. T.U. per la trasparenza nelle P.A. → pubblicazione nei siti istituzionali delle PP.AA. dei documenti e dei dati concernenti l'organizzazione e l'attività amministrativa, cui corrisponde il diritto di chiunque di accedere direttamente al sito, senza autenticazione ed identificazione.
Dipartimento della Funzione Pubblica → circolare n. 2/2013 → l'attuazione della trasparenza deve essere contemperata con l'interesse costituzionalmente protetto della tutela della riservatezza. Nel disporre la pubblicazione le P.A. → adottare tutte le cautele necessarie per evitare un'indebita diffusione di dati personali, consultando gli orientamenti del Garante per la protezione dei dati personali per ogni caso di dubbio → principi generali di non eccedenza e pertinenza nel trattamento, di cui all'art. 11 D. Lgs. 196/2003, e alcune previsioni dello stesso D.Lgs. 33/2013 (ad esempio, il ricorso all'anonimizzazione dei dati personali, richiesto dall'art. 4 per la pubblicazione sul sito di dati che le PP.AA. dispongono di pubblicare pur non essendone obbligate).
DUE CASI PROBLEMATICI DI RICHIESTA DI ACCESSO. La richiesta di accesso agli elaborati scritti di tutta la classe in caso di contestazione della valutazione attribuita all'alunno (Consiglio di Stato 7650/2010). La richiesta di accesso da parte del controinteressato alla documentazione prodotta per usufruire dei benefici della L.104/92 (Tar Campania 1029/2010 – No; Tar Puglia 3789/2010 - Sì).
ESEMPIO DI PROVVEDIMENTO DEL GARANTE SULLA PUBBLICAZIONE DI DATI. Tutto ciò premesso, il Garante, ritenuto illecito il trattamento dei dati effettuato dal Liceo Statale Farnesina di Roma nei termini indicati in premessa, ai sensi degli artt. 143, c. 1, lett. c) e 154, c. 1, lett. d), del Codice, vieta al Liceo Statale Farnesina di Roma di diffondere ulteriormente i nominativi dei propri studenti distinti per classe sul proprio sito Internet istituzionale, in assenza di una norma di L. o di regolamento che ammetta tale operazione di trattamento. Ai sensi degli artt. 152 del Codice e 10 del d.lgs. n. 150/2011 avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria.
SENTENZA 28 OTTOBRE 2010 N. 7650 - CONSIGLIO DI STATO – DIRITTO DI ACCESSO E PRIVACY. Con la sentenza n. 13135 del 2009 il Tar del Lazio, sede di Roma, ha accolto in parte il ricorso proposto dai genitori del minore (omissis) per l'annullamento dell'atto di diniego del DS del Liceo classico statale (omissis), relativo alla richiesta di accesso agli elaborati scritti del proprio figlio e degli altri compagni di classe (IV ginnasio) nelle materie di inglese, italiano, greco e matematica, oltre che ai registri personali delle insegnanti delle citate materie.
Il giudice di primo grado ha limitato l'accoglimento all'istanza degli interessati di accedere agli elaborati concernenti il proprio figlio, oltre ai registri di classe, mentre ha respinto la richiesta di accesso alle copie di tutti i compiti svolti dall'intera classe, nel presupposto che l'interesse diretto dei ricorrenti si concretizza esclusivamente nella tutela della posizione del proprio figlio, mentre l'analisi degli elaborati degli altri studenti della classe costituisce un raffronto di situazioni disomogenee tra loro e di scarsa utilità per l'interesse azionato.
2. La sentenza è appellata dagli originari ricorrenti, i quali si dolgono che ivi si dispone il "rilascio di copia" degli atti, anziché affermare il loro diritto di "prendere visione" degli originali ed eventualmente estrarre copia degli atti rilevanti; che

l'accesso agli atti degli altri studenti dovrebbe essere consentito eventualmente con mascheratura del nome o in forma anonima; che sussiste l'interesse a verificare se vi sia stata disparità di trattamento del proprio figlio attraverso il raffronto con i compiti scritti dei compagni di classe.
L'appello non può essere accolto.
Ai sensi dell'art. 39 dell'O.M. 21.5.2001 n. 90, il diritto di accesso ai documenti scolastici si esercita "mediante esame e visione degli atti, senza alcun pagamento, o con rilascio di copie conformi con rimborso del costo di produzione…".
La disposizione ministeriale consente, con l'uso della congiunzione disgiuntiva, entrambe le forme di accoglimento della richiesta di accesso e la spesa per le copie è così irrisoria da non ledere nessun diritto.
E' quindi infondata la censura che l'ufficio scolastico avrebbe dovuto consentire la previa visione degli atti. Inoltre il Collegio rileva che, ai sensi dell'art. 24, c. 3, della L. n. 241 del 1990, "non sono ammissibili istanze di accesso preordinate ad un controllo generalizzato dell'operato delle pubbliche amministrazioni".
Nel caso concreto, la richiesta di accesso agli elaborati di tutti i compagni di classe appare proprio un inammissibile controllo generalizzato, solo che si consideri che la funzione docente non è diretta alla scelta dei più meritevoli secondo una graduatoria di valore, bensì alla formazione dei ragazzi e alla verifica dei risultati da ognuno di essi conseguiti. Non si tratta pertanto di una procedura comparativa, nella quale potrebbe ipotizzarsi una disparità di trattamento. In concreto, poi, i voti molto negativi ottenuti dal minore in quasi tutte le materie, sia nella pagella del primo trimestre, sia in quella intermedia del marzo 2009 (allegati n. 5 e 6 del giudizio di primo grado), dimostrano l'inutilità della richiesta rispetto all'interesse diretto, concreto ed attuale dei genitori che si concretizza, come opportunamente affermato dal giudice di primo grado, "esclusivamente nella tutela della posizione del figliolo".
5. In conclusione la sentenza appellata resiste alle censure e va confermata.
Sussistono giusti motivi per l'integrale compensazione delle spese di lite, in considerazione della sostanziale assenza di difesa dell'Amministrazione.
Depositata in segreteria il 28/10/2010.
PROVVEDIMENTO GARANTE 20 DICEMBRE 2012 N. 431 – DIRITTO DI ACCESSO DELLE ORGANIZZAZIONI SINDACALI. L'Amministrazione non può trasmettere alle organizzazioni sindacali i dati relativi alle prestazioni di lavoro straordinario in forma nominativa, potendo soltanto procedere alla comunicazione di dati numerici o aggregati in forma anonima, salvo che il Contratto collettivo applicabile preveda espressamente che la comunicazione debba avere ad oggetto anche i dati nominativi del personale. Sui limiti al potere del contratto collettivo di precedere tale forma di comunicazione, il Garante rinvia al proprio provvedimento del 14 giugno 2007 (Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico).
Il Garante per la protezione dei dati personali accoglie il ricorso e per l'effetto dispone nei confronti del Ministero della giustizia, Dipartimento dell'amministrazione penitenziaria, il blocco dell'ulteriore comunicazione dei dati personali relativi alle prestazioni di lavoro straordinario del ricorrente alle organizzazioni sindacali, cui andrà altresì comunicato il presente provvedimento al fine di interdire l'ulteriore circolazione dei dati dello stesso tipo precedentemente comunicati. …

DIDATTICA A DISTANZA E PRIVACY – ESEMPIO DI REGOLAMENTO D'ISTITUTO. Informativa ai sensi dell'art. 13 del Regolamento UE 2016/679 (GDPR) relativa ai trattamenti di dati connessi alle attività di didattica a distanza

Titolare del trattamento

Titolare del trattamento è l'Istituto nel suo complesso, legalmente rappresentato dal DS.

Finalità del trattamento e tipologia di dati trattati

I dati personali sono trattati dal titolare per lo svolgimento delle funzioni istituzionali dell'Ente, che consistono nell'erogazione di un servizio pubblico di istruzione nei modi previsti dalle vigenti leggi e regolamenti, e nello svolgimento delle attività connesse. In particolare, la presente informativa è relativa ai trattamenti di dati connessi alle attività di didattica a distanza. I principali tipi di dati trattati sono i seguenti: credenziali di accesso alla piattaforma di didattica a distanza, indirizzo ip di collegamento, riprese fotografiche e filmiche dei partecipanti alla sessione di formazione a distanza, domande e risposte a domande, commenti vocali, commenti tramite chat, eventuali voti assegnati da parte del docente.

Base giuridica del trattamento

In generale, la base giuridica del trattamento risiede nell'art. 6 c. 1 lettera e) del GDPR, in quanto il trattamento è effettuato da un soggetto pubblico ed è necessario per lo svolgimento delle funzioni istituzionali; per quanto riguarda il trattamento di categorie particolari di dati personali, la base giuridica risiede nell'art. 9 c. 2 lettere b) e g). Relativamente alle attività di didattica a distanza, la base giuridica è costituita dall'art. 6 c. 1 lettera a) del GDPR.

Natura obbligatoria o facoltativa del conferimento dei dati e conseguenze del mancato conferimento dei dati

Il conferimento dei dati da parte dell'interessato assume carattere di obbligatorietà per poter erogare o per poter usufruire del servizio di didattica a distanza. Il mancato conferimento dei dati o il mancato consenso comporta l'impossibilità di usufruire dei servizi di formazione a distanza. Accedendo alla piattaforma di formazione a distanza l'utente (docente, genitore, alunno) fornisce implicitamente il consenso al trattamento dei dati.

Ambito di comunicazione dei dati

Lo svolgimento delle operazioni di trattamento comporta che i dati possano venire comunicati o portati a conoscenza da parte di soggetti esterni all'ente, che possono agire in regime di autonoma titolarità oppure essere designati in qualità di responsabili del trattamento. I dati personali raccolti sono altresì trattati dal personale del titolare, che agisce sulla base di specifiche istruzioni fornite in ordine a finalità e modalità del trattamento medesimo. In particolare per quanto riguarda le attività di didattica a distanza, i dati personali (comprese riprese fotografiche o filmiche) dei partecipanti, potranno essere portati a conoscenza di ciascuno degli altri partecipanti alla sessione di formazione a distanza. I dati forniti potranno essere comunicati a soggetti terzi con i quali siano in essere contratti o accordi di servizi finalizzati alla fruizione da parte degli interessati dei servizi stessi.

Tempo di conservazione dei dati

I dati verranno conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID … ed in ogni caso per un periodo non eccedente quello indispensabile per il perseguimento delle finalità.

Responsabile della protezione dei dati
Il Responsabile della Protezione dei Dati (RPD) è il Dott. , raggiungibile alla mail
Diritti degli interessati
Gli interessati hanno il diritto di ottenere dal titolare, nei casi previsti, l'accesso ai dati personali e la rettifica o la cancellazione degli stessi o la limitazione del trattamento che li riguarda o di opporsi al trattamento (artt. 15 e ss. del Regolamento). L'apposita istanza è presentata contattando il Responsabile della protezione dei dati, Dott.
Diritto di reclamo
Gli interessati che ritengono che il trattamento dei dati personali a loro riferiti avvenga in violazione di quanto previsto dal GDPR hanno il diritto di proporre reclamo al Garante, come previsto dall'art. 77 del Regolamento stesso, o di adire le opportune sedi giudiziarie (art. 79 del Regolamento).
Norme di comportamento
Si ricorda agli studenti ed ai genitori che anche nell'ambito delle attività di didattica a distanza sono tenuti a rispettare le norme previste in tema di privacy e le norme di comportamento di seguito riportate.
Lo studente e la famiglia si impegnano pertanto:
a conservare in sicurezza e mantenere segreta la password personale di accesso alla piattaforma di didattica a distanza, e a non consentirne l'uso ad altre persone;
a comunicare immediatamente attraverso email all'Istituto l'impossibilità ad accedere al proprio account scolastico, il sospetto che altri possano accedervi, ed episodi come lo smarrimento o il furto della password;
a non consentire ad altri, a nessun titolo, l'utilizzo della piattaforma di didattica a distanza;
a non diffondere, attraverso qualunque canale, eventuali informazioni riservate di cui venissero a conoscenza, relative all'attività delle altre persone che utilizzano il servizio;
ad osservare le presenti norme di comportamento, pena la sospensione da parte dell'Istituto dell'account personale dello studente e l'esclusione dalle attività di didattica a distanza e dai progetti correlati;
ad utilizzare i servizi offerti esclusivamente per le attività didattiche della Scuola;
a non diffondere in nessun modo in rete le attività realizzate dal docente, con il docente e i compagni;
a non diffondere in nessun modo screenshot o fotografie relative alle attività di didattica a distanza.
Il docente, lo studente e la sua famiglia si assumono la piena responsabilità di tutti i dati inoltrati, creati e gestiti attraverso la piattaforma di didattica a distanza.
Accedendo alla piattaforma di formazione a distanza, l'utente (docente, genitore, alunno) fornisce implicitamente il consenso al trattamento dei dati.
Il Garante ha infine ricordato alcune Faq.
Il docente, per il tramite delle piattaforme utilizzate per la didattica digitale, può mettere a disposizione degli studenti materiali didattici (anche proprie video lezioni) per la consultazione e i necessari approfondimenti da parte degli alunni e che, invece, non è ammessa la videoregistrazione della lezione a distanza nel corso della quale si manifestano le dinamiche di classe. Ciò in quanto l'utilizzo delle piattaforme deve essere funzionale a ricreare lo spazio virtuale in cui si esplica la

relazione e l'interazione tra il docente e gli studenti, non diversamente da quanto accade nelle lezioni in presenza.
Quando la creazione di un account personale è necessaria per l'utilizzo di piattaforme per la DDI, il trattamento dei dati personali, riconducibile alle funzioni istituzionalmente assegnate alle scuole, è ammesso a condizione che vengano attivati i soli servizi strettamente necessari allo svolgimento dell'attività didattica: in tali casi non deve essere richiesto il consenso dell'utente (studente, genitore o docente) o la sottoscrizione di un contratto.
GLI ERRORI RELATIVI ALLA PRIVACY NELLA NOTA MIUR SULLA DIDATTICA A DISTANZA – MARZO 2020. L'ultima nota del Ministero dell'Istruzione, la nr. 388 del 17 marzo 2020, fornisce le prime indicazioni operative per la didattica a distanza. L'atto in questione è una "nota" ministeriale, operativa in ambito di didattica a distanza, formalmente non qualificata come "circolare", pur avendone tutti i contenuti. Se "nota" di certo è solo indicativa, può essere disattesa dagli uffici cui si rivolge, possibilmente con un'adeguata motivazione. Anche se volessimo definirla "circolare" non muta di fatto la conclusione. Una circolare ministeriale può avere varie funzioni. La "circolare" di cui discutiamo può essere definita organizzativa, per taluni aspetti anche interpretativa, in ogni caso di certo non può produrre effetti al di fuori dell'Amministrazione emanante e, come da insegnamento delle sentenze Cass. SSUU n. 23031/2007 e Consiglio di Stato n. 7521/2010, può comunque essere disattesa dagli uffici della stessa Amministrazione con un'adeguata motivazione. Ad una circolare non può quindi essere riconosciuta alcuna efficacia normativa esterna rispetto all'Amministrazione emanante e non può essere annoverata fra gli atti generali di imposizione in quanto essa non può né contenere disposizioni derogative di norme di L., né essere considerata al pari di una norma regolamentare vera e propria.
In relazione alla questione privacy, la nota in esame chiarisce che le scuole non hanno bisogno di raccogliere il consenso dei genitori o degli alunni maggiorenni per fornire i servizi di didattica a distanza. Questa è senz'altro uno dei compiti istituzionali della scuola e la modalità diversa di esplicazione – virtuale e non in presenza- non ne inficia la natura. Fin qui, nulla quaestio, salvo poi specificare (tra parentesi) che il consenso le scuole lo avrebbero dovuto raccogliere a inizio anno scolastico. Su tale aspetto, occorre ricordare che il 99% delle attività di trattamento delle pubbliche amministrazioni non ha e non può avere come "base giuridica" il consenso, bensì l'esecuzione di compiti di intesse pubblico, l'adempimento a obblighi di L. (come specifica dall'art. 2-ter del D. Lgs. 196/2003 – Codice Privacy) e, semmai vi fosse un trattamento di categorie particolati di dati, i "motivi di interesse pubblico rilevante" (che ne caso specifico è il diritto all'istruzione – art. 2 sexies, c. 2lett. bb del D. Lgs. 196/2003 – Codice Privacy).
A supportare questa osservazione c'è l'art. 6 del regolamento UE 2016/679, declinato dai citati articoli del D. Lgs. 196/03 sugli aspetti Italiani, ma anche il considerando 43, che ne illustra la ratio, e l'autorevole linea guida sul consenso pubblicata dal Comitato Europeo per la Protezione dei Dati.
Alcuni ritengono che nessuna delle attività svolte dalla scuola nell'esercizio dei suoi compiti istituzionali di interesse pubblico possano in alcun modo essere assoggettate a consenso, contrariamente a quanto indicato dal MIUR nella nota.
Questione atti di nomina a responsabile esterno

Le criticità del contenuto della nota si manifestano soprattutto subito dopo, quando il MIUR, con una sintesi sin troppo veloce e fuorviante, ricorda alle scuole gli obblighi del GDPR, in tre punti.
Il primo riprende i principi generali in materia, quali la liceità, la correttezza, la trasparenza e la sicurezza del trattamento.
Il secondo punto riguarda la necessità di "stipulare contratti o atti di individuazione del responsabile del trattamento ai sensi dell'art. 28 del Regolamento, che per conto delle stesse tratta i dati personali necessari per l'attivazione della modalità didattica a distanza". In altre parole, secondo il Ministero dell'Istruzione, tutti i fornitori delle piattaforme o degli strumenti utilizzati dai docenti per la didattica a distanza devono essere nominati, con atto formale, responsabili esterni del trattamento. Ma non si è detto, nelle precedenti comunicazioni, che alle scuole è lasciata la più ampia libertà nella scelta degli strumenti da utilizzare?
Ricordiamo che le scuole sono ricorse a una serie di soluzioni, da quelle più "professionali" come Microsoft 365 o GSuite For Education, a piattaforme generalmente utilizzate per scopi personali come Whatsapp, Telegram, finanche strumenti opensource come Jitsi.
Il MIUR ci sta dicendo che dobbiamo trasmettere a Facebook (proprietario del servizio Whatsapp), Google o Skype un atto formale firmato digitalmente dal DS di nomina a responsabile del trattamento? E in quale lingua, inglese? Ed in virtù di quale vincolo i suddetti soggetti dovrebbero assoggettare i loro servizi, sistematicamente e tipicamente rivolti ai singoli individui e quindi erogati in qualità di titolari del trattamento, alle disposizioni di un ente pubblico italiano?
E' vero anche che molte software house che forniscono già alle scuole gli applicativi di contabilità, personale o Registro elettronico si sono attrezzate, implementando i loro servizi e mettendo a disposizione alcune piattaforme per la didattica a distanza. In questo caso può essere ragionevole (in quanto gli stessi fornitori degli applicativi agiscono già in qualità di responsabili del trattamento per l'archiviazione dei dati degli alunni sui loro server) estendere il relativo atto di nomina anche a questa nuova attività di trattamento; sempre che, ovviamente, i servizi siano erogati in tal senso e sotto il controllo dell'Istituto Scolastico. Se invece sono integrati con altre piattaforme web i cui fruitori sono le singole persone fisiche, anche le piattaforme integrate agiranno come soggetti indipendenti e la scuola potrà solo rendere debita informativa agli utilizzatori.
Infine, il punto tre: le scuole sono tenute a "sottoporre i trattamenti dei dati personali coinvolti a valutazione di impatto ai sensi dell'art. 35 del regolamento [Reg. UE 679/2016]" (c.d. DPIA- Data Protection Impact Assessment)
L'art. citato del Regolamento europeo dispone che il titolare, prima di avviare un trattamento che può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, operi una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. In altre parole, l'obbligo di effettuare una DPIA è conseguente alla presenza di un rischio elevato per i diritti e le libertà delle persone (che in questo caso sono gli studenti ed i docenti), che i trattamenti specificati possano comportare. Il GDPR elenca i casi nei quali è necessario procedere alla DPIA, ovvero:
• trattamenti che comportino una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato,

compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
• trattamenti, su larga scala, di categorie particolari di dati personali (come i dati relativi alla salute, all'orientamento sessuale, all'appartenenza religiosa ecc.) di dati relativi a condanne penali e a reati;
• trattamenti che operino la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.
Il Garante per la Protezione dei Dati italiano, con provvedimento n. 467 del 1 ottobre 2018, ha meglio specificato tutti i trattamenti che debbono essere sottoposti a DPIA, ovvero:
• valutativi o di scoring su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche on-line o attraverso app, relativi ad "aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato";
… • su larga scala di dati aventi carattere estremamente personale, ovvero dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali i dati finanziari);
• effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti;
• non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo), ma solo su "larga scala";
• effettuati attraverso l'uso di tecnologie innovative …;
• di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. mobile payment);
• di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10;
• sistematici di dati biometrici…;
Dall'elenco sopra indicato si evince come alcun trattamento rientri nell'obbligo per le scuole di effettuare una valutazione d'impatto sulla protezione dati in quanto:
• non può applicarsi il concetto di larga scala a una scuola che opera su un territorio limitato;
• le piattaforme utilizzate non si basano su nuove tecnologie innovative (quali l'IoT, i sistemi di intelligenza artificiale, l'utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale, monitoraggi effettuati da dispositivi wearable, tracciamenti di prossimità come ad es. il Wi-Fi tracking, etc.);
• attraverso la FaD e la DaD non si realizza alcun trattamento di categorie particolari di dati.
Da ultimo, ma non da meno, è importante ricordare che il rischio dipende dalle attività effettuate: se quindi gli istituti scolastici, effettuando la valutazione del rischio, che comunque è obbligatoria per L., stabiliscono misure di comportamento e di

protezione adeguate a proteggere gli studenti (ed in particolare i minori) dai rischi di utilizzo dei dati personali che transitano nei sistemi di DAD e FAD, il rischio elevato non si configura in alcun modo.
Dunque, vi sono almeno tre considerazioni da fare in ordine alla nota MIUR, circa la necessità di sottoporre a DPIA il trattamento connesso alla didattica a distanza.
La prima: in quale, tra l'esaustivo elenco di trattamenti "rischiosi" fornito dal Garante, rientrerebbe la didattica a distanza?
La seconda: perché il Ministero non aveva mai, prima d'ora, indicato tale necessità, pur essendo, la didattica a distanza, in uso in numerose scuole da diverso tempo (pensiamo a quelle che l'hanno attivata per i ragazzi costretti a casa o a ricoveri ospedalieri di lungo termine)?
TRATTAMENTO DI DATI RELATIVI ALLA VACCINAZIONE ANTI COVID-19 NEL CONTESTO LAVORATIVO (da riconsiderare dopo la decisione di rendere obbligatorio il Green pass per il personale scolastico e di incaricare del controllo i Dirigenti scolastici – agosto 2021). Il datore di lavoro non può chiedere ai propri dipendenti di fornire informazioni sul proprio stato vaccinale o copia di documenti che comprovino l'avvenuta vaccinazione anti Covid-19. Ciò non è consentito dalle disposizioni dell'emergenza e dalla disciplina in materia di tutela della salute e sicurezza nei luoghi di lavoro. Il datore di lavoro non può considerare lecito il trattamento dei dati relativi alla vaccinazione sulla base del consenso dei dipendenti, non potendo il consenso costituire in tal caso una valida condizione di liceità in ragione dello squilibrio del rapporto tra titolare e interessato nel contesto lavorativo (considerando 43 del Regolamento).
Il medico competente non può comunicare al datore di nominativi dei dipendenti vaccinati. Solo il medico competente può infatti trattare i dati sanitari dei lavoratori e tra questi, se del caso, le informazioni relative alla vaccinazione, nell'ambito della sorveglianza sanitaria e in sede di verifica dell'idoneità alla mansione specifica (artt. 25, 39, c. 5, e 41, c. 4, d.lgs. n. 81/2008). Il datore di lavoro può invece acquisire, in base al quadro normativo vigente, i soli giudizi di idoneità alla mansione specifica e le eventuali prescrizioni e/o limitazioni in essi riportati (es. art. 18 c. 1, lett. c), g) e bb) d.lgs. n. 81/2008).
La vaccinazione anti Covid-19 dei dipendenti può essere richiesta come condizione per l'accesso ai luoghi di lavoro e per lo svolgimento di determinate mansioni (ad es. in ambito sanitario)? Nell'attesa di un intervento del legislatore nazionale che, nel quadro della situazione epidemiologica in atto e sulla base delle evidenze scientifiche, valuti se porre la vaccinazione anti Covid-19 come requisito per lo svolgimento di determinate professioni, attività lavorative e mansioni, allo stato, nei casi di esposizione diretta ad "agenti biologici" durante il lavoro, come nel contesto sanitario che comporta livelli di rischio elevati per i lavoratori e per i pazienti, trovano applicazione le "misure speciali di protezione" previste per taluni ambienti lavorativi (art. 279 nell'ambito del Titolo X del d. lgs. n. 81/2008).
In tale quadro solo il medico competente, nella sua funzione di raccordo tra il sistema sanitario nazionale/locale e lo specifico contesto lavorativo e nel rispetto delle indicazioni fornite dalle autorità sanitarie anche in merito all'efficacia e all'affidabilità medico-scientifica del vaccino, può trattare i dati personali relativi alla vaccinazione dei dipendenti e, se del caso, tenerne conto in sede di valutazione dell'idoneità alla mansione specifica. Il datore di lavoro dovrà invece limitarsi ad

attuare le misure indicate dal medico competente nei casi di giudizio di parziale o temporanea inidoneità alla mansione cui è adibito il lavoratore (art. 279, 41 e 42 del d.lgs. n.81/2008).

GESTIONE DEGLI INDIRIZZI MAIL DEL PERSONALE SCOLASTICO E PRIVACY.

Esistono due tipi di mail, quella strettamente personale, e quella che ha l'estensione ministeriale che corrisponde al domicilio informatico del dipendente con tutte le conseguenze del caso.

Il Garante della Privacy con doc. web n. 8159221 n. 53 del 1° febbraio 2018 si è pronunciato sulla disciplina lavoristica in materia di mail. Pur riguardando il pronunciamento la gestione privatistica nel rapporto di lavoro, i principi come applicati, possono essere estesi anche alla P.A.

La raccolta sistematica delle comunicazioni elettroniche in transito sugli account aziendali dei dipendenti in servizio, la loro memorizzazione per un periodo non predeterminato e comunque, allo stato, amplissimo e la possibilità per il datore di lavoro di accedervi per finalità indicate in astratto e in termini generali - quali la difesa in giudizio o il perseguimento di un legittimo interesse - consente alla società di effettuare il controllo dell´attività dei dipendenti. Ciò risulta in contrasto con la disciplina di settore in materia di controlli a distanza (cfr. artt. 11, c. 1, lett. a) e 114 del Codice e art. 4, L. 20.5.1970, n. 300). Tale disciplina infatti, pure a seguito delle modifiche disposte con l´art. 23 del D. Lgs. 14 settembre 2015, n. 151, non consente l´effettuazione di attività idonee a realizzare il controllo massivo, prolungato e indiscriminato dell´attività del lavoratore (v. Linee guida per posta elettronica e internet citate in premessa, spec. par. 4, 5.2. lett. b) e 6; Consiglio di Europa, Raccomandazione del 1 aprile 2015, CM/Rec(2015)5, spec. princ. 14). Inoltre il datore di lavoro, pur avendo la facoltà di verificare l´esatto adempimento della prestazione lavorativa ed il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, deve in ogni caso salvaguardarne la libertà e la dignità (v., tra gli altri, Provv. n. 139 del 7 aprile 2011, doc. web n. 1812154; Provv. n. 308 del 21.7.2011, doc. web n. 1829641; Provv. 23 dicembre 2010, doc. web n. 1786116; si veda in proposito Cass. 31.3.2016, n. 13057, laddove si afferma che qualora "siano attivate caselle di posta elettronica – protette da password personalizzate – a nome di uno specifico dipendente, quelle «caselle» rappresentano il domicilio informatico proprio del dipendente […]. La casella rappresenta uno «spazio» a disposizione – in via esclusiva – della persona, sicché la sua invasione costituisce, al contempo, lesione della riservatezza"). Tanto più che l´assenza di una esplicita policy al riguardo può determinare una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione (cfr. Linee guida per posta elettronica e internet, cit., spec. 3; 5.2. lett. b), e 6.1.).

All'atto della cessazione del rapporto di lavoro la mail lavorativa va disattivata.

Con riferimento ai trattamenti effettuati sulla posta elettronica aziendale dopo la cessazione del rapporto di lavoro, come già precisato dal Garante in precedenti occasioni, in conformità ai principi in materia di protezione dei dati personali, gli account riconducibili a persone identificate o identificabili devono essere rimossi previa disattivazione degli stessi e contestuale adozione di sistemi automatici volti ad informarne i terzi ed a fornire a questi ultimi indirizzi alternativi riferiti all'attività professionale del titolare del trattamento.

L’indirizzo mail personale è riservato. Nelle linee guida del 2 marzo 2011 il Garante ha inoltre precisato che non si possono riprodurre sul web i dati sullo stato di salute, i cedolini dello stipendio, l’orario di entrata e di uscita, l’indirizzo privato, la e-mail personale. Che è diversa da quella professionale. “Non appare giustificato riprodurre sul web informazioni quali i cedolini dello stipendio, dati di dettaglio risultanti dalle dichiarazioni fiscali, oppure riguardanti l´orario di entrata e di uscita di singoli dipendenti, l´indirizzo del domicilio privato, il numero di telefono e l´indirizzo di posta elettronica personale (diversi da quelli ad uso professionale), ovvero informazioni attinenti allo stato di salute di persone identificate, quali le assenze verificatesi per ragioni di salute.”
Le linee guida del Garante per posta elettronica. Con provvedimento numero 13 del 1° marzo 2007 Lavoro: le linee guida del Garante per posta elettronica e internet pubblicato sulla Gazzetta Ufficiale n. 58 del 10 marzo 2007 ha espresso, invece, alcuni principi importanti proprio sula questione della posta elettronica. Il contenuto dei messaggi di posta elettronica – come pure i dati esteriori delle comunicazioni e i file allegati– riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui ratio risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un’ulteriore protezione deriva dalle norme penali a tutela dell´inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto c., c.p.; art. 49 Codice dell’amministrazione digitale).
Tuttavia, con specifico riferimento all’impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all´indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell´organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.
La mancata esplicitazione di una policy al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione. Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all’indirizzo di posta elettronica usato dal lavoratore (posta “in entrata”) o di quelli inviati da quest’ultimo (posta “in uscita”).
É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell’attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull´eventuale segretezza della corrispondenza.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore;

- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le “coordinate” (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l’apertura della posta elettronica. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi webmail), il titolare del trattamento, perdurando ´assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l’amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati), l´attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all´attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l´interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l´eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell´organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta policy datori

Regolamentazione utilizzo mail, dal PTOF, al contratto integrativo ai regolamenti interni. Con tutte le garanzie del caso, come richiamate dal garante, per quanto riguarda la modalità di utilizzo e diffusione della mail lavorativa, sarebbe opportuno disciplinarne il corretto utilizzo ad esempio nel PTOF. L’art. 3 del regolamento di cui al decreto del Presidente della Repubblica 8 marzo 1999, n. 275, afferma che ogni istituzione scolastica predispone, con la partecipazione di tutte le sue componenti, il piano triennale dell’offerta formativa, rivedibile annualmente. Il piano è il documento fondamentale costitutivo dell’identità culturale e progettuale delle istituzioni scolastiche ed esplicita la progettazione curricolare, extracurricolare, educativa e organizzativa che le singole scuole adottano nell’ambito della loro autonomia. Ad esempio si possono prevedere le modalità di comunicazione tra “utenza” e personale scolastico. Così come è importante che ogni scuola provveda a dotarsi di un proprio regolamento sul punto. Ma affinché sia il più condiviso possibile dalla comunità scolastica è bene che si armonizzi con quanto contemplato dall’art. 22 lettera c8 e c 9 del CCNL scuola. Lettere che in materia di contrattazione integrativa riguardano i criteri generali per l’utilizzo di strumentazioni tecnologiche di lavoro in orario diverso da quello di servizio, al fine di una maggiore conciliazione tra vita lavorativa e vita familiare (diritto alla disconnessione); i riflessi sulla qualità del lavoro e sulla professionalità delle innovazioni tecnologiche e dei processi di informatizzazione inerenti ai servizi amministrativi e a supporto dell’attività scolastica.

Utilizzo indirizzario mail per comunicazioni sindacali. Anche la questione dell'utilizzo della mail per finalità sindacali sarebbe bene definirlo all'interno dell'istituzione scolastica. Certamente esiste l'albo sindacale, la bacheca sindacale, strumenti idonei a soddisfare le esigenze della pubblicità sindacale. Ma anche gli indirizzari mail professionali resi pubblici potrebbero essere utilizzati. Anche in questo caso soccorrono alcune interpretazioni giurisprudenziali che concernano il settore privato. Il provvedimento del Tribunale di Catania, Sezione Lavoro, 2 febbraio 2009. Tornando alle attività sindacali effettuate con i mezzi informatici ed alla riconduzione delle stesse a quelle tradizionali indicate dallo Statuto dei lavoratori, deve ritenersi che l'attività invio o di ricezione di comunicazioni sindacali attraverso la posta elettronica possa equipararsi all'attività di volantinaggio, che rientra nell'ambito della libertà sindacale concessa a qualunque organizzazione presente in azienda non vedendosi in cosa consista la differenza tra la materiale consegna ai dipendenti di volantini stampati sul luogo di lavoro e l'invio agli stessi, anche sulla loro posta elettronica aziendale, di una email avente identico contenuto – attività di volantinaggio che, come noto, è di per sé lecita in quanto non arrechi pregiudizio alla normale attività aziendale. (vedasi Pretura di Torino, sentenza del 18 marzo 1995, Estensore Cambria).
Diversamente avverrebbe per il caso di utilizzo dell'indirizzo di posta elettronica aziendale per ricevere e/o inviare messaggi privati, condotta che costituisce, invece senza dubbio, un illecito contrattuale, considerato che possono ribadirsi per la posta elettronica le argomentazioni già elaborate dalla giurisprudenza con riferimento all'uso per utilità propria o di terzi di altri strumenti di lavoro, quali il telefono, il computer o internet. Posto, dunque, alla stregua di quanto sopra, che deve ritenersi pienamente lecita l'attività di invio di comunicazioni sindacali a mezzo di e-mail, anche quando essa sia diretta a indirizzi aziendali di posta elettronica, nei limiti in cui la stessa, per le modalità con le quali viene esercitata, non sia idonea ad arrecare pregiudizio, intralciandola, alla normale attività aziendale, deve rilevarsi che, nel caso di specie – alcun dubbio essendovi, anche alla stregua della stessa contestazione di addebito mossa al dipendente dalla società resistente, che le comunicazioni contestate abbiano contenuta e natura prettamente sindacale – appare rispettato il limite suddetto, in quanto il mero invio di una e-mail ad un dipendente dell'impresa è di per se priva di ogni invasività della sua sfera lavorativa, dipendendo, in buona sostanza, non dalla modalità di trasmissione in se, ma dalla responsabile condotta del lavoratore ricevente il fatto che la comunicazione sia letta in orario di lavoro, con illecita distrazione del lavoratore."

Il Tribunale di Milano con provvedimento del 10 maggio del 2002 sosteneva un concetto similare, come anche quello di Foggia, il 10 luglio del 2000 riconoscendo che l'utilizzo, della mail aziendale per le informazioni di carattere sindacale ai lavoratori è certamente da considerarsi espressione del tradizionale diritto di affissione di cui all'art. 25 dello Statuto dei lavoratori. Che così recita: Le rappresentanze sindacali aziendali hanno diritto di affiggere, su appositi spazi, che il datore di lavoro ha l'obbligo di predisporre in luoghi accessibili a tutti i lavoratori all'interno dell'unità produttiva, pubblicazioni, testi e comunicati inerenti a materie di interesse sindacale e del lavoro.

L’utilizzo della mail rientra nel tempo lavoro. Può sembrare una cosa da niente, ma sta prendendo piede, in modo non regolamentato, e senza freno, l’abitudine di comunicare via mail questioni di servizio quando non si è in orario di lavoro, e neanche in servizio, per non parlare delle mail che possono pervenire da alcune famiglie verso l’indirizzo istituzionale mai del docente, in qualsiasi momento del giorno. D’altronde un docente, quando può rispondere alla mail? Sicuramente non mentre presta servizio in classe. Risponderà, così come avviene, di norma, in quello che sarebbe il suo tempo libero, che viene spesso impiegato per preparare il suo lavoro a scuola, dalla correzione dei compiti, alla preparazione delle verifiche, tempo di lavoro non riconosciuto e non retribuito. Anche l’utilizzo della mail per fini lavorativi rientra nel tempo lavoro ed il diritto alla disconnessione che è stato contrattualizzato proprio per queste ragioni e va definito all’interno dei paletti della contrattazione d’istituto, come in precedenza richiamato.

LA NOMINA DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (D.P.O). Il Regolamento generale per la protezione dei dati personali n. 2016/679 (General Data Protection Regulation o GDPR) è la normativa europea in materia di protezione dei dati. Il Regolamento è stato pubblicato sulla Gazzetta Ufficiale europea il 4 maggio 2016, è entrato in vigore il 24 maggio 2016, ma la sua attuazione è avvenuta a distanza di due anni, quindi a partire dal 25 maggio 2018.

Trattandosi di un regolamento, non necessita di recepimento da parte degli Stati dell’Unione ed è attuato allo stesso modo in tutti gli Stati dell’Unione senza margini di libertà nell’adattamento (tranne per le parti per le quali si prevede espressamente delle possibilità di deroga). Il suo scopo è, infatti, la definitiva armonizzazione della regolamentazione in materia di protezione dei dati personali all’interno dell’Unione europea. Questo perché col Trattato di Lisbona la protezione dei dati personali è diventata diritto fondamentale dei cittadini, e quindi va garantito allo stesso modo in tutto il territorio dell’Unione.

L’art. 39 del Regolamento generale sulla protezione dei dati (GDPR) afferma che i compiti del DPO includono:

- informare e consigliare il responsabile del trattamento o il responsabile del trattamento e i dipendenti che eseguono il trattamento dei loro obblighi ai sensi del presente regolamento e di altre […] disposizioni sulla protezione dei dati;
- monitorare la conformità al presente regolamento, ad altre […] disposizioni in materia di protezione dei dati e alle politiche del titolare del trattamento o del responsabile del trattamento in relazione alla protezione dei dati personali, compresa l’assegnazione di responsabilità, la sensibilizzazione e la formazione del personale coinvolto nelle operazioni di trattamento e relativi audit;
- fornire consulenza, ove richiesto, per quanto riguarda la valutazione d’impatto sulla protezione dei dati e monitorarne le prestazioni […];
- collaborare con l’autorità di controllo;
- fungere da punto di contatto per l’autorità di controllo su questioni relative al trattamento […] e consultare , se del caso, in merito a qualsiasi altra questione. “

In termini più semplici, il DPO deve:

- assicurarsi che le attività scolastiche si svolgano nel rispetto del GDPR;

- raccogliere informazioni sulle attività di elaborazione dei dati della scuola;
- analizzare e verificare che le attività di elaborazione dati della scuola siano conformi;
- consigliare il personale in merito alla conformità delle attività al GDPR.

Formazione

- garantire che tutto il personale scolastico coinvolto nell'elaborazione dei dati sia adeguatamente formato;
- istruire tutto il personale scolastico sui requisiti di conformità al GDPR;

Contatto

- fungere da punto di contatto tra la scuola e le autorità di controllo del GDPR;
- comunicare con gli interessati per informarli su come vengono utilizzati i loro dati.

Il GDPR richiede che il DPO agisca in modo indipendente e autonomo. È quindi importante che si abbia il pieno supporto e l'assistenza del DS.

E' anche necessario collaborare con il personale ATA della scuola che gestisce i dati personali su base giornaliera. Ciò può includere:

- gestori di rete;
- rapporti con il DSGA;
- responsabili della ristorazione;
- personale docente (in particolare i fiduciari di plesso e, in primis, i collaboratori del DS).

Come punto di partenza, è una buona idea iniziare a verificare i meccanismi attualmente in atto in relazione ai dati personali nella scuola. È necessario eseguire una serie di controlli in modo da poter rispondere alle seguenti domande:

- Dove vengono archiviati i dati personali della tua scuola?
  Ad esempio, può essere archiviato in archivi, sistemi di messaggistica di posta elettronica, dischi rigidi di computer o registratori video e audio.
- Come vengono utilizzati i dati personali nella scuola?
  Come vengono raccolti e registrati i dati; per quanto tempo vengono conservati i dati; quando verranno cancellati i dati; qual è la base giuridica per il trattamento dei dati? In che modo la tua scuola raccoglie e registra il consenso (ove richiesto) all'uso dei dati?
- La scuola dispone di una politica sulla protezione dei dati? Questo è seguito da tutto il personale?
  Considera se il personale della tua scuola memorizza e utilizza correttamente i dati personali. Ad esempio, se la politica di conservazione dei dati della scuola prevede di conservare i dati personali di un alunno per un anno dopo che ha lasciato la scuola, questa politica viene seguita?
- Vengono segnalate violazioni dei dati?
  Quale formazione è attualmente offerta al personale scolastico sulla protezione dei dati? Questa formazione è stata registrata? La scuola offre corsi online sulla protezione dei dati, giornate di formazione, ecc.? La scuola ha una registrazione di tutta la formazione sulla protezione dei dati? Tutto il personale della scuola ha compreso l'importanza di rispettare le leggi sulla protezione dei dati?

E' necessario considerare tutto il personale: dal DS agli addetti alle pulizie. È buona norma tenere un registro delle risposte alle domande precedenti. Le prove sono utili

per gli audit e anche durante le indagini se si verifica effettivamente una violazione dei dati.
ATTACCO INFORMATICO E DATA BREACH A SCUOLA: VALUTAZIONE DELLE VIOLAZIONI DI DATI O SISTEMI. Lo scopo di questa procedura è quello di definire gli elementi che caratterizzano una violazione di dati personali al fine di:

- riconoscere una violazione;
- valutare le conseguenze;
- valutare gli adempimenti derivanti;
    - comunicazione al garante;
    - comunicazione agli interessati;
- valutare le misure di sicurezza da correggere o adottare.

La valutazione, da parte del DS, deve essere effettuata rapidamente, prevedibilmente entro 72 ore dalla sua consapevolezza.
Se la violazione avviene sui sistemi affidati ad un responsabile, questi ne informa il Titolare "senza ingiustificato ritardo". Da quel momento, e non dal verificarsi della violazione, decorreranno le 72 ore per la valutazione e la eventuale segnalazione.
Riconoscere che si è verificata una violazione. È quindi necessario riconoscere innanzitutto il tipo di violazione:

- accesso abusivo a dati personali e violazione dei sistemi di sicurezza;
- distruzione, perdita o modifica dei dati;
- divulgazione non autorizzata dei dati.

Il concetto di "perdita" necessita di un approfondimento. Secondo il Garante: con "perdita" dei dati personali si dovrebbe invece intendere il caso in cui i dati potrebbero comunque esistere, ma il titolare del trattamento potrebbe averne perso il controllo o l'accesso, oppure non averli più in possesso.
Nelle "Linee guida sulla notifica delle violazioni – GDPR" si L. all'art. 33 Notifica di una violazione dei dati personali all'autorità di controllo: "In caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'art. 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo".

Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo. Il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione.
La notifica deve:

- descrivere la natura della violazione dei dati personali compresi, ove possibile, le categorie e il numero approssimativo di interessati in questione nonché le categorie e il numero approssimativo di registrazioni dei dati personali in questione;
- comunicare il nome e i dati di contatto del responsabile della protezione dei dati o di altro punto di contatto presso cui ottenere più informazioni;
- descrivere le probabili conseguenze della violazione dei dati personali;

- descrivere le misure adottate o di cui si propone l'adozione da parte del titolare del trattamento per porre rimedio alla violazione dei dati personali e anche, se del caso, per attenuarne i possibili effetti negativi.

Qualora e nella misura in cui non sia possibile fornire le informazioni contestualmente, le informazioni possono essere fornite in fasi successive senza ulteriore ingiustificato ritardo.

Il titolare del trattamento documenta qualsiasi violazione dei dati personali, comprese le circostanze a essa relative, le sue conseguenze e i provvedimenti adottati per porvi rimedio. Tale documentazione consente all'autorità di controllo di verificare il rispetto del presente art..

Comunicazione di una violazione dei dati personali all'interessato. Quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo.

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

- il titolare del trattamento ha messo in atto le misure tecniche e organizzative adeguate di protezione e tali misure erano state applicate ai dati personali oggetto della violazione, in particolare quelle destinate a rendere i dati personali incomprensibili a chiunque non sia autorizzato ad accedervi, quali la cifratura;
- il titolare del trattamento ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati;
- detta comunicazione richiederebbe sforzi sproporzionati. In tal caso, si procede invece a una comunicazione pubblica o a una misura simile, tramite la quale gli interessati sono informati con analoga efficacia.

Nel caso in cui il titolare del trattamento non abbia ancora comunicato all'interessato la violazione dei dati personali, l'autorità di controllo può richiedere, dopo aver valutato la probabilità che la violazione dei dati personali presenti un rischio elevato, che vi provveda.

Tipi di violazione. Le violazioni possono esser classificate in base a tre principi:

- "violazione della riservatezza", in caso di divulgazione dei dati personali o accesso agli stessi non autorizzato o accidentale;
- "violazione dell'integrità", in caso di modifica non autorizzata o accidentale dei dati personali;
- "violazione della disponibilità", in caso di perdita, accesso o distruzione accidentali o non autorizzati di dati personali.

La valutazione della violazione della disponibilità può avere elementi di indeterminatezza. Una perdita o una distruzione permanenti dei dati saranno sempre considerate violazioni della disponibilità. Tuttavia, come possiamo considerare la indisponibilità temporanea?

Afferma il Garante che: nell'attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, si dovrebbe prendere in considerazione, tra le altre cose, "la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di

trattamento" e "la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico".
Di conseguenza, un incidente di sicurezza che determina l'indisponibilità dei dati personali per un certo periodo di tempo costituisce una violazione, in quanto la mancanza di accesso ai dati può avere un impatto significativo sui diritti e sulle libertà delle persone fisiche.
Valutazione dell'impatto. Dunque, anche un evento che ci ha privato temporaneamente della disponibilità dei dati deve comportare una valutazione dell'impatto che può avere avuto sui diritti e sulle libertà delle persone, così come una perdita di disponibilità definitiva, un accesso non autorizzato o la diffusione non controllata.
Risulta quindi fondamentale che il titolare, e in alcuni casi prima di lui il responsabile, ne venga a conoscenza tempestivamente.
Non tutte le violazioni attiveranno la necessità di notificare al Garante o agli interessati, ma senz'altro tutte dovranno essere annotate nei loro elementi salienti così come dovranno essere annotate le valutazioni in base alle quali verranno prese le decisioni successive.
Procedura di valutazione delle violazioni. È possibile suddividere la procedura di valutazione delle violazioni nelle seguenti fasi:

- riconoscimento del sussistere della violazione
- comunicazione degli elementi da valutare
- annotazione sul registro
- valutazione degli elementi
- eventuale notifica al Garante
- eventuale notifica agli interessati
- completamento dell'annotazione sul registro
- eventuale indicazione di nuove misure di sicurezza e loro verifica.

DOCUMENTO DI INDIRIZZO DEL GARANTE SU DESIGNAZIONE, POSIZIONE E COMPITI DEL RESPONSABILE DELLA PROTEZIONE DEI DATI (RPD) IN AMBITO PUBBLICO. Con nota prot. AOODPPR RU n. 1317 del 03/12/2021, il Capo del Dipartimento per le risorse umane, finanziarie e strumentali del MI ha invitato le Direzioni generali a diffondere il Documento di indirizzo in oggetto presso le Istituzioni scolastiche dei territori di competenza. Tale documento, consultabile al link https://www.gpdp.it/web/guest/home/docweb/ - /docweb - display/docweb/9589104 e adottato dall'Autorità Garante per la protezione dei dati personali con provvedimento n. 186 de l 29 aprile 2021, pubblicato sulla Gazzetta Ufficiale n. 132 del 4 giugno c.a., fornisce importanti indicazioni per l'individuazione del RPD.
"Tenuto conto– si L. nella sopra richiamata nota del Capo Dipartimento - che le istituzioni scolastiche, per numero di soggetti coinvolti e per qualità e quantità di servizi offerti alle famiglie e agli altri utenti di riferimento, sono, in ambito pubblico, tra i principali attori titolari di trattamenti di dati personali ... si pone quale elemento indispensabile per il governo delle complessità connesse ... la designazione di un RPD adeguatamente qualificato, supportato da sufficienti risorse e in una posizione di indipendenza rispetto alla sfera decisionale del titolare".
Il tema, di particolare importanza anche al fine di migliorare la qualità delle valutazioni connesse al trattamento dei dati personali e rendere più efficace i

rapporti con il Garante competente in materia, è stato oggetto di approfondimento nel corso della Giornata della Trasparenza per le scuole 2021.