General
Data
Protection
Regulation

(regolamento europeo sulla protezione dei dati)

VADEMECUM PER LA SCUOLA

Istituto Comprensivo

BENIAMINO GIGLI

Recanati

SOMMARIO

Riferimenti **3**

Obiettivi **3**

Principi generali **4**

Diritti degli interessati **6**

Ruolo del DPO **7**

Come contattare il DPO 7

Applicazioni pratiche in ambito scolastico **8**

Azioni potenzialmente pericolose **8**

FAQ - Frequently Asked Questions **11**

Come possiamo gestire G-Suite for Education di Google? 11

Possiamo utilizzare un canale YouTube privato? 11

Possiamo pubblicare sulla pagina Facebook della scuola? 11

È corretto creare un gruppo WhatsApp con i genitori per le comunicazioni con le famiglie? 11

Possiamo utilizzare le mail degli studenti composte con il nome e il cognome (ad esempio nome.cognome@istituto.org)? 11

Possiamo utilizzare un'unica liberatoria per più finalità (es. foto/video per recite, immagini televisive, giornali ecc.)? 11

È possibile comunicare gli elenchi con i nominativi degli studenti ad altre scuole per l'orientamento in modo che le altre scuole possano inviare loro del materiale informativo? 11

Alcuni Enti Pubblici come l'UMEE inviano per posta elettronica nominativi di famiglie e di studenti che sono necessarie per le certificazioni DSA o H. Come devono essere trattati questi dati? 12

Come possiamo condividere tra docenti la documentazione relativa ai PDP? 12

Come possiamo condividere la documentazione relativa ai PDP con le famiglie? 12

Come devono essere gestite le foto appese in classe o per i corridoi? 12

Come gestire il video fatto da una maestra che riprende la festa della scuola, che poi consegna alla famiglia? 12

Le certificazioni di lingua sono pubblicate dalla società che se ne occupa, con nominativi e risultati. Come vanno gestite? 12

Come si gestisce il fatto che i nominativi dei ragazzi confluiscono in progetti Regionali o in piattaforme per la scuola alternanza lavoro del ministero? 12

È possibile effettuare il caricamento sul sito della scuola di immagini dei ragazzi senza consenso? 13

Posso proibire l'utilizzo del cellulare a scuola? 13

Di fronte a un genitore che a voce mi dice che sono modificati i termini dell'affidamento condiviso, devo modificare il modo di agire dell'istituto? 13

È conforme al Regolamento la pubblicazione sul sito istituzionale dei dati dei minori? 13
È vietato pubblicare l'elenco degli alunni sul sito della scuola? 13
Come devono essere gestite la ripresa di immagini e le registrazioni a scuola? 13
Come devono essere gestiti i questionari per attività di ricerca? 14
L'informativa è proprio necessaria? 14
Le scuole non possono pubblicare graduatorie on line con dati personali e sensibili? 14
Come provvedo all'obbligo di informativa privacy quando effettuo le Prove INVALSI? 14
Come devo gestire l'indicizzazione dei motori di ricerca (come Google) del sito web istituzionale? E dell'Albo Pretorio? 14
È necessario bilanciare le disposizioni sulla trasparenza con quelle in materia di privacy? 15
Quali sono gli obblighi di pubblicazione per finalità di trasparenza? 15
Le Scuole possono pubblicare qualunque dato e informazione personale per finalità di trasparenza? 15
Quali sono i limiti agli obblighi di pubblicazione online di atti e documenti contenenti dati personali? 15
Cosa deve fare una Scuola prima di pubblicare un documento? 16
Quali dati personali non vanno pubblicati online? 16
Si possono diffondere dati ulteriori rispetto a quelli per i quali è prevista la pubblicazione obbligatoria? 16
Come si attua l'anonimizzazione? 16
È prevista una durata della pubblicazione? 16
Come deve essere gestita la pubblicazione dei curricula professionali? 16
È corretto comunicare o diffondere i nominativi dei docenti che percepiscono il cosiddetto bonus? 17

Appendici **18**
Allegato 1 - Il linguaggio della Protezione dei dati 18
Allegato 2 – Esempi di Data breach 20
Allegato 3 – Gestione delle immagini 21
Allegato 4 – Azioni e condizioni di liceità / rischi / accortezze necessarie 22
Allegato 5 – Commento alle piattaforme gratuite come di Google 24

Riferimenti

Al fine di aiutare il lettore nell'accesso ai materiali, sono forniti numerosi collegamenti ai materiali disponibili in rete, che sono stati accuratamente valutati dal Team DPO, non richiedono registrazioni di sorta e sono liberamente scaricabili.

TEMA	LINK AL MATERIALE
Applicazione del GDPR	https://www.garanteprivacy.it/regolamentoue/guida-all-applicazione-del-regolamento-europeo-in-materia-di-protezione-dei-dati-personali
Scuola	https://www.garanteprivacy.it/scuola
Cyberbullismo	https://www.garanteprivacy.it/cyberbullismo
Smart Toys	https://www.garanteprivacy.it/iot/smarttoys
Social privacy	https://www.garanteprivacy.it/garante/document?ID=3140059
e-state in privacy	https://www.garanteprivacy.it/estate
Ransomware	https://www.garanteprivacy.it/ransomware
Droni	https://www.garanteprivacy.it/droni
Phishing	https://www.garanteprivacy.it/phishing
App	http://www.garanteprivacy.it/app

Obiettivi

Le ragioni alla base della scelta del legislatore europeo nell'introduzione della figura di Responsabile della protezione dei dati che sorvegli l'osservanza del G.D.P.R., provveda alla sensibilizzazione e alla formazione del personale che effettua trattamenti di dati personali, si possono sintetizzare in:

a) compiere un intervento prima di tutto culturale;
b) lavorare sulla consapevolezza delle persone rispetto ai rischi connessi con i trattamenti soprattutto se informatizzati e peggio se effettuati on-line;
c) localizzare l'Autorità Garante (o potenzialmente la sua influenza) presso ogni Titolare;
d) semplificare l'applicazione normativa con personale specificatamente dedicato;
e) facilitare la divulgazione delle modifiche e integrazioni normative;
f) demistificare il Regolamento grazie a un approccio normativo innovativo e rivolto più alla sostanza che alla forma.

Principi generali

Per facilitare la vita al lettore e per una migliore comprensione del tema, abbiamo inserito uno specifico capitolo sui principi ispiratori del Regolamento e sui diritti degli interessati.
In questa prima parte riportiamo, per così dire, la teoria e nella seconda parte del vademecum sono invece illustrate le applicazioni pratiche.
I principi applicabili al trattamento di dati personali sono riportati all'art. 5 del Regolamento:

PRINCIPIO	DESCRIZIONE
Liceità *art. 5 Lettera a)*	I dati personali devono essere trattati in modo lecito, corretto e trasparente nei confronti dell'interessato. Le condizioni di liceità previste sono: - Esecuzione di un contratto - Obbligo legale - Interesse pubblico - Legittimo interesse - Salvaguardia degli interessi vitali dell'interessato - Consenso Se non sono presenti almeno una delle precedenti condizioni, il trattamento è illecito e il Titolare soggetto a sanzioni. Il concetto di trasparenza si concretizza con l'informativa, che deve riportare tutta una serie di informazioni utili per fare in modo che l'interessato possa esplicitare i propri diritti.
Limitazione della finalità *art. 5 Lettera b)*	I dati personali possono essere raccolti solo per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità.
Minimizzazione dei dati o anche privacy by default *art. 5 Lettera c)*	I dati personali devono essere adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati. Il Titolare del trattamento mette in atto misure tecniche e organizzative adeguate a garantire che siano trattati, per impostazione predefinita, solo i dati personali necessari per ogni specifica finalità del trattamento.
Esattezza dei dati *art. 5 Lettera d)*	I dati personali devono essere esatti e aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati.
Limitazione della conservazione art. 5 Lettera e)	I dati personali sono conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati (applicazione nella PA del massimario di conservazione/scarto)
Integrità e riservatezza art. 5 Lettera f)	I dati personali sono trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali. Durante tutto il ciclo di vita del trattamento, è necessario garantire un livello di protezione adeguato ai dati personali.
Responsabilizzazione o	Il Titolare del trattamento deve rendere conto delle azioni fatte o fatte

accountability art. 5 Comma 2	fare, rispondere e rendere conto dei risultati ottenuti, delle cose fatte (fatte bene e fatte male).

Altri principi generali applicabili alla protezione dei dati personali:

PRINCIPIO	DESCRIZIONE
Prevenzione	L'organizzazione dovrebbe avere un approccio proattivo piuttosto che reattivo attuando tutta una serie di misure di prevenzione adeguate ai rischi connessi con il trattamento dei dati.
Privacy by design	La protezione dei dati dovrebbe essere attuata sin dalla progettazione partendo dalla regola "tutto negato, a meno degli autorizzati".
Protezione adeguata ai rischi	Cambio di paradigma, da sistema-centrico (come il vecchio D.lgs. 196/03) a data-centrico: non più indicazioni tecniche o misure minime, superate in poco tempo dall'innovazione tecnologica ma principi generali sempre applicabili. Il Titolare valuta i rischi e attua tutte le misure che ritiene necessarie ad evitare il danno.
Centralità dell'interessato	Prima di tutto i diritti, la dignità e la libertà delle persone.

Diritti degli interessati

Tutto il personale scolastico è chiamato a trattare non solo i dati personali dei ragazzi ma anche delle famiglie, dei colleghi e in alcuni casi dei fornitori di beni e servizi.

Il concetto di *accountability* o responsabilizzazione tende a rovesciare il vecchio paradigma di un'unica autorità garante della protezione dei dati e 60 milioni tra vittime e carnefici, trasformando tutti coloro che trattano dati in veri e propri "garanti" di quanto elaborato e gestito.

Questa (pseudo) inversione comporta tutta una serie di vantaggi a patto che i diritti degli interessati (le persone di cui stiamo trattando i dati) conoscano e possano esplicitare quanto previsto dal GDPR, di seguito riportato per completezza:

ARTICOLI	DIRITTI DEGLI INTERESSATI
Art. 7	Diritto alla prestazione e revoca del consenso
Art. 12	Diritto alla trasparenza
Artt. 13, 14	Diritto all'informazione
Art. 15	Diritto di accesso ai dati personali e di proporre reclamo all'autorità di controllo
Art. 16	Diritto di rettifica
Art. 17	Diritto di cancellazione o Diritto all'oblio (*)
Art. 18	Diritto di limitazione del trattamento (*)
Art. 20	Diritto alla portabilità dei dati (*)
Art. 21	Diritto di opposizione (*)
Art. 22	Diritto di non essere sottoposti ad una decisione automatizzata e alla profilazione
Art. 34	Diritto di ricevere informazioni in ordine alla violazione dei propri dati personali

(*) Diritti non applicabili ai trattamenti di dati personali necessari per l'esecuzione di compiti di interesse pubblico o connessi all'esercizio di pubblici poteri.

È disponibile sul sito web istituzionale il Modulo di richiesta di accesso ai dati personali da parte dell'interessato per gli adempimenti previsti dagli articoli 15, 16, 17, 18, 20, 21 del GDPR.

Ruolo del DPO

Il Responsabile della Protezione dei dati o DPO, come previsto all'art. 39, è la nuova figura introdotta dal GDPR che:

- ➔ Informa e fornisce consulenza a chi effettua trattamenti
- ➔ È il punto di contatto per l'Autorità Garante
- ➔ Coopera con l'Autorità di controllo
- ➔ Fornisce pareri sulla DPIA
- ➔ Sorveglia l'osservanza del GDPR

Si pone al centro rispetto al Titolare, gli Interessati (allievi, famiglie, personale docente e non docente, fornitori) e l'Autorità Garante, come il ruolo del pivot nel basket.
Oltre alle necessarie competenze rispetto alla tematica della protezione dei dati, è necessaria una visione completa del settore specifico di applicazione e della relativa disciplina di settore, costantemente informato sulle novità legislative e sulla prassi.
Inoltre, visto l'elevato grado di informatizzazione dei processi sono necessarie specifiche competenze tecniche in ambito informatico e in particolare rispetto a tutta la catena tecnologica.
Nella pratica, nessuno è in grado di racchiudere tutti questi aspetti a un livello adeguato ai rischi connessi con il trattamento dei dati. È per questo motivo che spesso la gestione del servizio di DPO è svolta da un gruppo che include esperti di sistemi di gestione, consulenti legali, tecnici informatici ed esperti in sicurezza delle informazioni.
La sua figura risulta di fondamentale importanza in caso di data breach, poiché non solo ha il compito istituzionale di tenere i contatti con l'Autorità Garante ma guida l'organizzazione nella gestione, documentazione, attenuazione e risoluzione dell'evento avverso.
La cosa importante da tener presente è che il DPO è a vostra completa disposizione per risolvere qualsiasi questione in ambito dati personali, aiutarvi nel percorso di evoluzione della sicurezza, consigliarvi le buone pratiche.
L'obiettivo comune è raggiungere la necessaria conformità normativa ed al contempo elevare il livello di sicurezza nel trattamento dei dati personali.

Come contattare il DPO

RESPONSABILE PROTEZIONE DATI: Morolabs Srl nella persona di Francesco Moroncini
Tel. / FAX: 071.9030585 / 071.2210025
e-mail / PEC: dpo@morolabs.it / morolabs@legalmail.it

Applicazioni pratiche in ambito scolastico

La prima cosa da fare, prima di effettuare un trattamento dei dati è porsi le seguenti domande:

1. Sto trattando dati personali? E di che tipo?
2. Posso danneggiare qualcuno, anche solo potenzialmente?
3. Qual è la reale finalità?
4. Cosa dice a riguardo il Regolamento interno sulla protezione dei dati?
5. Qual è la condizione di liceità prevista?
6. È possibile minimizzare, pseudonimizzare o anonimizzare alla fonte le informazioni raccolte?
7. È un nuovo trattamento? È già presente nel registro delle attività di trattamento?
8. Quali rischi corriamo come organizzazione… e come responsabilità personali?
9. Sono in grado di far applicare i diritti dell'interessato?
10. Ho applicato tutte le misure di sicurezza previste dal Titolare?

Azioni potenzialmente pericolose

A volte il buon senso non è sufficiente ad evitare il danno. Per questo motivo riportiamo una tabella riassuntiva delle azioni con i dati personali degli interessati che sono nel tempo risultate pericolose e a volte hanno provocato danni. Nella terza colonna sono riportati le possibili alternative e precauzioni:

AZIONI	RISCHI	ALTERNATIVE / PRECAUZIONI
WhatsApp per condivisione informazioni	diffusione backup non criptati su Google drive	solo strumenti istituzionali / file hosting istituzionale
Posta / Google drive per salvataggio documenti contenenti dati personali	diffusione salvataggio dati personali extra UE	criptazione / file hosting istituzionale
Pen drive personali per backup e condivisione	perdita Pen drive e diffusione dei contenuti	criptazione / file hosting istituzionale
Computer personali (a casa) per la memorizzazione / duplicazione dei dati	diffusione dei contenuti	applicazione policy di sicurezza / file hosting istituzionale
Condivisione degli account e delle	accesso abusivo ad un sistema	corretta definizione delle autorizzazioni

password tra utenti	informatico CP 615 ter	
Stessa password per tutti i servizi di istituto e personali	superficie di esposizione più ampia accesso abusivo	password anche leggermente diverse
Post-it con password appiccicata sul display	accesso abusivo	*brain training*
Scrivania come archivio	perdita / diffusione	armadi / archivi di deposito / evitare di stampare
Invio stampe su multifunzione di piano senza ritiro immediato	perdita / diffusione	Dematerializzazione o completamento transizione al digitale
Documenti nella spazzatura, al massimo accartocciati	diffusione	distruggi documenti (o almeno policy "strappa prima di buttare")
Riutilizzo della carta già stampata (con dati personali) per altre stampe	diffusione	dematerializzazione o completamento transizione al digitale
Invio di dati personali via mail (non istituzionale) senza criptazione	potenziale esportazione extra UE / diffusione	mail istituzionale / PEC / criptazione / "valigetta" / file hosting aziendale
Pubblicazione su Albo ON-LINE	diffusione dati personali senza condizione di liceità	Verifica puntuale/controlli/monitoraggio/ minimizzazione dei dati pubblicati (solo gli effettivamente necessari) evitare indicizzazione contenuti scaduti da più di 5 anni da parte dei motori di ricerca utilizzando il file Robots.txt
Pubblicazione su sito web istituzionale di registrazioni, riprese o immagini degli allievi	diffusione dati personali senza consenso interessati e liberatoria	Necessario specifico consenso al trattamento e la liberatoria ai sensi della tutela del diritto d'autore. La pubblicazione di materiali con minori di 14 anni deve avvenire con le dovute accortezze.
Pubblicazione sui social istituzionali di registrazioni, riprese o immagini degli allievi	diffusione dati personali senza consenso interessati e liberatoria	Necessario specifico consenso al trattamento e la liberatoria ai sensi della tutela del diritto d'autore. Da ricordare che i sistemi di riconoscimento facciale di alcuni social hanno potenzialità di correlazioni impressionanti
Collegamento della posta istituzionale sul proprio smartphone	salvataggio di dati personali su strumenti non tracciati e con politiche di protezione basate su privacy setting delle app	Utilizzare strumenti aziendali programmati per la possibilità in caso di smarrimento di un wipe-out da remoto. Eliminare mail e allegati (anche da download) quando non più necessari. In caso di dismissione del dispositivo provvedere ad una cancellazione a basso livello.
Password digitata senza le dovute accortezze	accesso abusivo ad un sistema informatico CP 615 ter	Utilizzare password complesse; digitare velocemente avendo cura di non essere osservati

Transazioni on-line	furto	Attivare le funzionalità di messaggio post transazione. Controllare spesso il conto. Verificare anche le piccole transazioni. Utilizzare solo siti sicuri con connessione https (barra indirizzo verde) Tenere poco denaro nel conto per acquisti on-line
Utilizzo dei Social Network	diffusione dati personali furto di identità furto	Non condividere troppe informazioni e non raccontate troppo della vostra vita Impostare correttamente le impostazioni privacy. Bloccate gli utenti sospetti. Non accettare amici casuali. Attivare autenticazione a doppio fattore. Essere consapevoli della reputazione on-line
Utilizzo dei sistemi on-line e dei Wi-Fi pubblici	furto di identità furto	Evitare transazioni sensibili su Wi-Fi pubblici. Usare le impostazioni privacy. Non dimenticare di fare log out. Non aprire mail da sconosciuti e non fare click sui link. Transazioni sensibili solo in https. Non scaricare file da siti sconosciuti o non sicuri. Utilizzare indirizzi di e-mail usa e getta per le registrazioni. Non salvare le password nei browser. Salvare i dati più sensibili localmente piuttosto che su file host remoti
Dopo un data breach	Può succedere di tutto…	Cambiare subito tutte le password. Non ignorare mail a tuo nome arrivate ad amici e colleghi. Riconosci i segnali ed evidenze del data breach. Riprendi il controllo dei tuoi dati. Scopri esattamente cosa ha provocato il problema

FAQ - Frequently Asked Questions

Come possiamo gestire G-Suite for Education di Google?

Oltre alle condizioni presenti nel contratto, Google afferma di rispondere ai requisiti del GDPR e di aver predisposto un percorso di conformità. Comunque, per l'iscrizione dei minori ai diversi servizi offerti, come Google Classroom, Drive, Gmail, YouTube è necessario chiedere il consenso alle famiglie e si consiglia di condividere solo i dati personali necessari all'iscrizione, evitando di pubblicare informazioni eccedenti. Da evitare la condivisione di documenti contenenti dati relativi alla salute, come i PDP.

Da ricordare inoltre che le condizioni previste da Google, come anche dal GDPR, per la gestione del consenso on-line degli allievi prevede un'età minima di 14 anni per l'Italia. [è disponibile un approfondimento in allegato]

Possiamo utilizzare un canale YouTube privato?

Qualora si intenda utilizzare un canale YouTube per fini scolastici è opportuno avvalersi di G-Suite for Education e, in caso di video dove sono ripresi i propri studenti, accertarsi che per ogni studente siano stati firmati consenso e liberatoria da parte dei genitori.

Possiamo pubblicare sulla pagina Facebook della scuola?

Una pagina Facebook della scuola invece non ha le stesse protezioni di Google e quindi, trattandosi di diffusione di dati personali, di possibile trattamento dati fuori UE, con la sola adesione agli accordi Usa-UE detti *shield*, va gestita con cautela e bisogna evitare di inserire dati personali e immagini dei ragazzi.

È corretto creare un gruppo WhatsApp con i genitori per le comunicazioni con le famiglie?

Le comunicazioni con WhatsApp, visto che i numeri delle rubriche e i dati potrebbero essere inviati fuori UE, sono sotto la responsabilità del singolo, il titolare del numero telefonico, che deve evitare di trattare dati personali senza autorizzazioni. Se il numero è intestato alla scuola, va richiesta un'autorizzazione per trattare i numeri di telefono delle famiglie e inviare solo comunicazioni che non trattino dati personali. Se il numero è del singolo soggetto deve chiedere l'autorizzazione per creare il gruppo.

Possiamo utilizzare le mail degli studenti composte con il nome e il cognome (ad esempio nome.cognome@istituto.org)?

Si, con consenso. L'importante poi è che venga utilizzata in un ambiente ristretto e non venga diffusa. Tra questi ambienti ci sono anche i portali dei libri, Aica, ecc.

È importante che nell'acquisizione del consenso venga comunicata la corretta informazione in merito all'utilizzo.

Possiamo utilizzare un'unica liberatoria per più finalità (es. foto/video per recite, immagini televisive, giornali ecc.)?

Si può fare, ma prevedendo la possibilità di scegliere se acconsentire singolarmente alle une o alle altre.

È possibile comunicare gli elenchi con i nominativi degli studenti ad altre scuole per l'orientamento in modo che le altre scuole possano inviare loro del materiale

informativo?

Senza consenso del ragazzo/genitore non è proprio possibile. È molto più semplice far arrivare direttamente alla scuola il materiale informativo e distribuirlo. Meno informazioni girano e meno rischi si corrono.

Alcuni Enti Pubblici come l'UMEE inviano per posta elettronica nominativi di famiglie e di studenti che sono necessarie per le certificazioni DSA o H. Come devono essere trattati questi dati?

L'UMEE dovrebbe almeno criptare la documentazione poiché la posta elettronica ha il livello di sicurezza equivalente a una "cartolina postale". Nel caso di invii non corretti, segnalate l'accaduto al DPO.

Come possiamo condividere tra docenti la documentazione relativa ai PDP?

La soluzione migliore è l'utilizzo del Registro o di sistemi di file hosting istituzionali. Se si vuole utilizzare la posta elettronica va utilizzata @istruzione.it avendo cura che i destinatari non effettuino re-invii (o *relay*) su altri indirizzi e in particolari su smartphone.

Nel caso non sia possibile o non vi sia la disponibilità degli strumenti, è necessario provvedere alla pseudonimizzazione (es. Rossi Mario = Paperino senza riportare nel documento ulteriori informazioni utili alla correlazione con l'interessato).

Come possiamo condividere la documentazione relativa ai PDP con le famiglie?

Devono essere attuate ulteriori accortezze come la criptazione degli allegati, avendo cura di comunicare su altro media la chiave di decriptazione (evitare di inviare una mail con riportata la frase "la chiave per decriptare l'allegato documento è…")

Come devono essere gestite le foto appese in classe o per i corridoi?

Nessun problema poiché rientrano in un ambito ristretto. Se non è eccessivamente gravosa, ad ogni modo, è sempre meglio avere sia la liberatoria che il consenso.

Come gestire il video fatto da una maestra che riprende la festa della scuola, che poi consegna alla famiglia?

Nessun problema in quanto è sempre un ambito ristretto. Se il genitore poi decide di diffonderlo su un social network, la responsabilità di quella diffusione resta in capo al genitore.

Le certificazioni di lingua sono pubblicate dalla società che se ne occupa, con nominativi e risultati. Come vanno gestite?

L'informativa della società che se ne occupa è necessaria e deve riportare le modalità di trattamento.

Come si gestisce il fatto che i nominativi dei ragazzi confluiscono in progetti Regionali o in piattaforme per la scuola alternanza lavoro del ministero?

Nell'informativa iniziale bisogna inserire che i dati personali comuni verranno comunicati in questi portali per obbligo di legge o adempimenti contrattuali. Nel caso dell'Alternanza Scuola-Lavoro, sarà la stessa azienda interessata, poi, che dovrà dare l'informativa ai genitori del minore su come tratterà i dati dei ragazzi.

È possibile effettuare il caricamento sul sito della scuola di immagini dei ragazzi senza consenso?

Può essere fatta solo oscurando/sfocando i volti o facendo delle foto "di contesto", che non rendano il soggetto direttamente identificabile come negli esempi presenti nell'Allegato 3.

Posso proibire l'utilizzo del cellulare a scuola?

Non si può costringere un ragazzo a non portare un cellulare a scuola. Si può prevedere nel Regolamento interno dell'Istituto che in classe ne sia vietato l'utilizzo durante l'orario di lezione.

Di fronte a un genitore che a voce mi dice che sono modificati i termini dell'affidamento condiviso, devo modificare il modo di agire dell'istituto?

No, al massimo si può chiedere di fornire un documento ufficiale da mettere agli atti che attesti quanto lo stesso sta dichiarando.

È conforme al Regolamento la pubblicazione sul sito istituzionale dei dati dei minori?

Le Scuole devono pubblicare on line solo dati la cui pubblicazione risulti realmente necessaria e prevista dalle norme. È sempre vietata la pubblicazione di dati sulla salute e sulla vita sessuale. I dati particolari (etnia, religione, appartenenze politiche etc.) possono essere diffusi solo laddove indispensabili al perseguimento delle finalità di rilevante interesse pubblico. Occorre adottare misure per impedire la indicizzazione dei dati delicati da parte dei motori di ricerca e il loro riutilizzo. Qualora si intendano pubblicare dati personali ulteriori rispetto a quelli individuati nel decreto legislativo n. 33/2013 sulla trasparenza, si deve procedere prima all'anonimizzazione di questi dati, evitando soluzioni che consentano l'identificazione, anche indiretta o a posteriori, dell'interessato.

È necessario pubblicare negli atti solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita.

È vietato pubblicare l'elenco degli alunni sul sito della scuola?

A decretarlo è il Garante per la protezione dei dati personali con il provvedimento n. 383 del 6 dicembre 2012, il quale ha sostenuto che "la diffusione da parte di un soggetto pubblico è ammessa unicamente quando prevista da una norma di legge o da un regolamento".

Pertanto, ha dichiarato "l'illiceità della diffusione di dati personali in esame, in quanto effettuata dal Liceo in assenza di una norma di legge o di regolamento che la ammetta".

Come devono essere gestite la ripresa di immagini e le registrazioni a scuola?

L'uso di cellulari e smartphones è in genere consentito per fini strettamente personali, ad esempio per registrare le lezioni, e sempre nel rispetto delle persone. Spetta, comunque, agli istituti scolastici

decidere nella loro autonomia come regolamentare o se vietare del tutto l'uso dei cellulari. Non si possono diffondere immagini, video o foto sul web se non con il consenso delle persone riprese. È bene ricordare che la diffusione di filmati e foto che ledono la riservatezza e la dignità delle persone può far incorrere lo studente in sanzioni disciplinari e pecuniarie, o perfino in veri e propri reati.

Stesse cautele vanno previste per l'uso dei tablet, se usati a fini di registrazione e non soltanto per fini didattici o per consultare in classe libri elettronici e testi on line.

Come devono essere gestiti i questionari per attività di ricerca?

L'attività di ricerca con la raccolta di informazioni personali tramite questionari da sottoporre agli studenti è consentita solo se ragazzi e genitori sono stati prima informati sugli scopi della ricerca, le modalità del trattamento e le misure di sicurezza adottate. Gli studenti e i genitori devono essere lasciati liberi di non aderire all'iniziativa.

L'informativa è proprio necessaria?

Le scuole devono rendere noto alle famiglie e ai ragazzi, attraverso un'adeguata informativa, quali dati raccolgono e come li utilizzano. Spesso le scuole utilizzano nella loro attività quotidiana dati particolari – come quelli riguardanti le origini etniche, le convinzioni religiose, lo stato di salute – anche per fornire semplici servizi, come ad esempio la mensa. È bene ricordare che nel trattare queste categorie di informazioni gli istituti scolastici devono porre estrema cautela, in conformità al regolamento sui dati sensibili adottato dal Ministero dell'istruzione. Famiglie e studenti hanno diritto di conoscere quali informazioni sono trattate dall'istituto scolastico, farle rettificare se inesatte, incomplete o non aggiornate.

Le scuole non possono pubblicare graduatorie on line con dati personali e sensibili?

Le scuole non possono pubblicare on line numeri di telefono, codice fiscale o indirizzo del personale della scuola. Tutte le graduatorie, sia di docenti che di ATA, devono essere ripulite dai dati personali. Il Garante della Privacy ha accertato, dopo una ricerca sui siti web scolastici, che tali dati erano stati resi, tra l'altro, indicizzabili, il che vuol dire che sono raggiungibili anche solo digitando il nome su Internet. Il Garante, con il provvedimento del 2 marzo 2011 n. 88 (Linee guida in materia di trattamento di dati personali contenuto anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web), ha stabilito che le graduatorie devono contenere solo i dati strettamente necessari all'individuazione del candidato: nome, cognome, punteggio e posizione in graduatoria. Tutti gli altri dati, come indirizzo, telefono, non possono essere diffusi, per evitare abusi, compreso il furto di identità.

Come provvedo all'obbligo di informativa privacy quando effettuo le Prove INVALSI?

L'INVALSI pubblica sul proprio sito l'informativa sul trattamento dei dati personali degli studenti coinvolti nelle prove nazionali.

L'informativa spiega le modalità delle prove cui saranno sottoposti gli studenti ed è indirizzata ai

genitori. Si ribadisce quanto già messo in atto nelle prove degli anni passati, cioè: uso delle etichette con i codici della scuola, del plesso, del livello di classe e sezione sui fascicoli contenenti i testi delle prove saranno apposte etichette recanti i codici identificativi della scuola, del plesso, del livello di classe frequentata, della sezione e dello studente.

Come devo gestire l'indicizzazione dei motori di ricerca (come Google) del sito web istituzionale? E dell'Albo Pretorio?

Esiste l'obbligo di "indicizzare" i contenuti pubblicati tramite motori di ricerca generalisti (es. Google) per garantire la dovuta trasparenza ma è limitato ai soli dati tassativamente individuati dalle norme in materia di trasparenza.

Devono essere sottratti all'indicizzazione i dati sensibili e giudiziari contenuti negli atti pubblicati nell'albo pretorio online, includendo *no index*, *no archive* del "*robot exclusion*

protocol".

Inoltre, nella sezione "Amministrazione trasparente" è necessario inserire un avvertimento generale con il quale si informa i visitatori che i dati personali pubblicati sono "riutilizzabili solo alle condizioni previste dalla normativa vigente sul riuso dei dati pubblici (…), in termini compatibili con gli scopi per i quali sono stati raccolti e registrati, e nel rispetto della normativa in materia di protezione dei dati personali".

Da tenere ben presente che è sempre valido il principio di pertinenza e non eccedenza, rispettare i limiti temporali previsti dalla normativa di riferimento o al massimo fino al raggiungimento dello scopo per il quale l'atto è stato adottato e i dati resi pubblici. Vale anche il principio inverso per cui se la finalità è stata raggiunta il documento deve essere de-pubblicato.

È necessario rendere non intelligibili i dati personali non pertinenti o, se sensibili o giudiziari, non indispensabili rispetto alle specifiche finalità di trasparenza della pubblicazione.

È necessario bilanciare le disposizioni sulla trasparenza con quelle in materia di privacy?

Sì. Con l'adozione di apposite Linee guida (provvedimento del 15 maggio 2014), il Garante è intervenuto proprio per assicurare l'osservanza della disciplina in materia di protezione dei dati personali nell'adempimento degli obblighi di pubblicazione sul web di atti e documenti.

Le linee guida hanno lo scopo di individuare le cautele che i soggetti pubblici sono tenuti ad applicare nei casi in cui effettuano attività di diffusione di dati personali sui propri siti web istituzionali per finalità di trasparenza o per altre finalità di pubblicità dell'azione amministrativa.

Quali sono gli obblighi di pubblicazione per finalità di trasparenza?

Sono quelli, indicati principalmente nel decreto trasparenza, che riguardano l'organizzazione e l'attività delle pubbliche amministrazioni. Comprendono, ad esempio: i dati relativi agli organi di indirizzo politico e di amministrazione e gestione; i dati sull'articolazione degli uffici, sulle competenze e sulle risorse a disposizione di ciascun ufficio, anche di livello dirigenziale non generale; i nomi dei dirigenti responsabili dei singoli uffici; l'illustrazione in forma semplificata dell'organizzazione dell'amministrazione (es. mediante l'organigramma); l'elenco dei numeri di telefono nonché delle caselle di posta elettronica cui il cittadino possa rivolgersi (avendo l'accortezza di mascherare l'indirizzo in modo che i bot non lo identifichino, ad esempio con nome (at) dominio.it).

Le Scuole possono pubblicare qualunque dato e informazione personale per finalità di trasparenza?

No. Vale la regola generale per la quale i soggetti pubblici possono diffondere dati personali solo se ciò è ammesso da una specifica disposizione di legge o di regolamento.

Quali sono i limiti agli obblighi di pubblicazione online di atti e documenti contenenti dati personali?

Dopo aver verificato la sussistenza dell'obbligo di pubblicazione dell'atto o del documento nel proprio sito web istituzionale, il soggetto pubblico deve limitarsi a includere negli atti da pubblicare solo quei dati personali realmente necessari e proporzionati alla finalità di trasparenza perseguita nel caso concreto.

Se sono sensibili (ossia idonei a rivelare ad esempio l'origine razziale ed etnica, le convinzioni religiose, le opinioni politiche, l'adesione a partiti o sindacati, lo stato di salute

e la vita sessuale) o relativi a procedimenti giudiziari, i dati possono essere trattati solo se indispensabili, ossia se la finalità di trasparenza non può essere conseguita con dati anonimi o dati personali di natura diversa.

Cosa deve fare una Scuola prima di pubblicare un documento?

Prima di procedere alla pubblicazione sul proprio sito web deve:

- individuare se esiste un presupposto di legge o di regolamento che legittima la diffusione del documento o del dato personale;
- verificare, caso per caso, se ricorrono i presupposti per l'oscuramento di determinate informazioni;
- sottrarre all'indicizzazione (cioè alla reperibilità sulla rete da parte dei motori di ricerca) i dati sensibili e giudiziari, come ricordato al punto precedente.

Quali dati personali non vanno pubblicati online?

È vietato diffondere dati personali idonei a rivelare lo stato di salute o informazioni da cui si possa desumere, anche indirettamente, lo stato di malattia o l'esistenza di patologie dei soggetti interessati, compreso qualsiasi riferimento alle condizioni di invalidità, disabilità o handicap fisici e/o psichici.

Il Garante ha più volte ribadito la necessità di garantire il rispetto della dignità delle persone, facendo oscurare, ad esempio, dai siti web di diversi Comuni italiani i dati personali contenuti nelle ordinanze con le quali i sindaci disponevano il trattamento sanitario obbligatorio per determinati cittadini.

Si possono diffondere dati ulteriori rispetto a quelli per i quali è prevista la pubblicazione obbligatoria?

No, a meno che tali dati non vengano resi effettivamente anonimi e non vi sia più la possibilità di identificare gli interessati, nemmeno indirettamente e in un momento successivo.

Come si attua l'anonimizzazione?

Per anonimizzare un documento non basta sostituire il nome e cognome con le iniziali dell'interessato ma occorre oscurare del tutto il nominativo e le altre informazioni riferite all'interessato che ne possono consentire l'identificazione anche a posteriori.

È prevista una durata della pubblicazione?

Sì. Il decreto trasparenza pone un termine generale di mantenimento online delle informazioni pari a 5 anni. È bene sottolineare che, in ogni caso, una volta raggiunti gli scopi per i quali i dati personali sono stati resi pubblici, gli stessi devono essere oscurati anche prima del termine dei 5 anni.

Come deve essere gestita la pubblicazione dei curricula professionali?

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 esempio, 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.

È corretto comunicare o diffondere i nominativi dei docenti che percepiscono il cosiddetto bonus?

Il nuovo contratto collettivo nazionale del comparto scuola prevede delle importanti modifiche per quanto riguarda l'aspetto della cd. "informazione successiva" prevista dal vecchio contratto.

In particolare, il vecchio contratto collettivo prevedeva all'art. 6 che fossero materia di informazione successiva sia i nominativi del personale utilizzato nelle attività e progetti retribuiti con il fondo d'istituto, sia la verifica dell'attuazione della contrattazione collettiva integrativa d'istituto sull'utilizzo delle risorse. Tale disposizione dava la possibilità, quindi, alle rappresentanze sindacali di accedere alle informazioni relative ai dati economici degli interessati rispetto al fondo d'istituto. Tale norma è stata utilizzata dagli organi giurisdizionali per dirimere le controversie fra istituti e rappresentanze sindacali a favore di queste ultime, in quanto vi era un elemento normativo espresso in questa direzione.

Diversamente con la stipula del contratto del comparto scuola sottoscritto nell'aprile 2018 non è più previsto l'istituto di informazione successiva per quanto riguarda i dati economici rispetto al fondo d'istituto in maniera analitica (del singolo soggetto).

Visto che sono oggetto di contrattazione integrativa i criteri di ripartizione delle risorse del fondo d'istituto saranno certamente da mettere a disposizione delle rappresentanze sindacali (a titolo di informazione, come relazione sindacale) i dati aggregati rispetto alla ripartizione delle risorse del predetto fondo, ma non i dati dei singoli interessati. Ciò è necessario per dare la possibilità alle rappresentanze sindacali di essere informati, per quanto di loro competenza, ai fini della contrattazione integrativa

In caso contrario, si eluderebbe la disciplina prevista dalla contrattazione collettiva e non essendoci, così, una base giuridica su cui fondare tale trattamento dei dati si potrebbe potenzialmente arrecare nocumento ai singoli interessati. Si realizzerebbe, pertanto, una comunicazione illegittima di dati riguardanti l'aspetto economico della persona e in quanto tali dati personali.

Le informazioni aggiornate sono disponibili sul sito web:

https://www.morolabs.it/scuole/faq-scuole-gdpr/

Appendici

Allegato 1 - Il linguaggio della Protezione dei dati

TERMINE	DESCRIZIONE	ESEMPIO
Dato	Sequenza di numeri e lettere non contestualizzati e quindi privi di significato	12345 Calcio
Informazione	Dati correlati tra di loro per ottenere un significato	Prezzo: € 12.345 Sport: Calcio Calcio: Ca
Interessato	Persona fisica identificata o identificabile	Maria Rossi (insegnante) Maria Rossini (allieva)
Dato personale	Qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»)	Maria Rossi è nata il 4.5.1967 Il suo stipendio lordo è di € 1.234
Dato particolare (sensibile) art. 9 GDPR	Dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché i dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona	Per gli allievi: H, DSA, BES, PEI, PDF, PDP foto con riportato evidente lo stato di salute di un allievo
Titolare	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali	L'istituzione scolastico nel suo complesso. Quando effettua trattamenti in combinazione con il MIUR, la scuola risulta essere contitolare del trattamento
Responsabile (esterno)	La persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del titolare del trattamento	Azienda fornitrice di software e servizi come il registro elettronico. Azienda che si occupa di catering
Registro delle attività di trattamento	Registro dove sono riportate tutte le informazioni utili alla protezione dei dati personali elaborati dall'organizzazione	È disponibile presso il Titolare per i controlli dell'Autorità Garante della protezione dei dati
Condizioni di Liceità del trattamento	Il trattamento è lecito solo se e nella misura in cui ricorre almeno una delle seguenti condizioni: 1. l'interessato ha espresso il consenso 2. trattamento necessario all'esecuzione di un contratto 3. trattamento necessario per adempiere un obbligo legale 4. trattamento necessario per la salvaguardia	Scuola dell'obbligo Contratto di lavoro con il personale Consenso al trattamento dei dati per immagini e riprese

	degli interessi vitali 5. trattamento necessario per l'esecuzione di un compito di interesse pubblico 6. trattamento necessario per il perseguimento del legittimo interesse del titolare	
Data Retention	Tempistiche di conservazione delle informazioni limitate a quanto necessario per raggiungere le finalità del trattamento. Al termine del periodo di conservazione dei dati, è necessario implementare adeguate procedure di smaltimento.	"Conserviamo le informazioni per il tempo necessario secondo quanto previsto dal massimario di scarto" Dopo 10 anni, distruggiamo tutti i compiti in classe e cancelliamo i dati riferiti ai genitori dei ragazzi.
Informativa	Informazioni previste agli artt. 13 e 14 da fornire agli interessati	Disponibile sul sito web dell'Istituto anche in modalità slide animata
Richiesta Accesso ai Dati	Modalità di esercizio dei diritti previsti per gli interessati	Disponibile sul sito web dell'Istituto
Data Protection Impact Assessment (DPIA)	Valutazione d'impatto sulla protezione dei dati Modalità di analisi dei rischi per gli interessati	Effettuata solo per trattamenti a rischio elevato
Data breach	Violazione dei dati personali che può, se non affrontata in modo adeguato e tempestivo, provocare danni fisici, materiali o immateriali alle persone fisiche, ad esempio perdita del controllo dei dati personali che li riguardano o limitazione dei loro diritti, discriminazione, furto o usurpazione d'identità, perdite finanziarie, decifratura non autorizzata della pseudonimizzazione, pregiudizio alla reputazione, perdita di riservatezza dei dati personali protetti da segreto professionale o qualsiasi altro danno economico o sociale significativo alla persona fisica interessata.	Smarrimento penna USB contente dati personali degli allievi Pubblicazione di elenchi di allievi sul sito web Invio di e-mail contente dai personali a destinatario errato
DPO/RPD	Data Protection Officer o Responsabile della protezione dei dati Figura deputata a: 1. informare e fornire consulenza 2. sorvegliare l'osservanza del regolamento 3. fornire parere su DPIA 4. cooperare con l'autorità di controllo 5. fungere da punto di contatto per l'autorità di controllo	Morolabs Srl

Allegato 2 – Esempi di Data breach

Tipo/Natura della violazione	Descrizione della violazione	Dati personali violati	Numero di interessati colpiti
Pubblicazione su sito web istituzionale	Pubblicazione elenchi studenti nel sito web (indicizzazione motori di ricerca avvenuta e oblio non attivo)	Nome e cognome allievi, classe e plesso di assegnazione	Allievi e famiglie classi prime
Numero di registrazioni dei dati colpite	Conseguenze della violazione	Gli interessati sono stati informati?	Azioni volte al contenimento della violazione dei dati e alla minimizzazione dell'impatto sugli interessati
300	I dati dal sito web istituzionale sono stati rimossi ma permangono informazioni su motore di ricerca Google	Una mamma ha informato la DS	Eliminazione contenuti web e comunicazione a Google secondo procedura standard prevista
Pubblicazione su sito web istituzionale	Pubblicazione elenchi (graduatoria ATA I fascia) assistente amministrativo e nel sito web (avvenuta indicizzazione motori di ricerca) con riportati indirizzi di residenza e numeri di telefono	residenza e numeri di telefono	200
Numero di registrazioni dei dati colpite	Conseguenze della violazione	Gli interessati sono stati informati?	Azioni volte al contenimento della violazione dei dati e alla minimizzazione dell'impatto sugli interessati
200	I dati dal sito web istituzionale sono stati rimossi e non è più possibile raggiungerli. Alcuni siti di indicizzazione hanno ancora il documento	Considerata la tipologia di dati pubblicati e la difficoltà nel raggiungere il documento, non sono stati informati gli interessati	Eliminazione contenuti web. Richiesta deindicizzazione dai motori

Allegato 3 – Gestione delle immagini

L'innovazione tecnologica, soprattutto se applicata agli smartphone, ha fatto passi da gigante negli ultimi 5 anni. Questi dispositivi permettono risoluzioni inimmaginabili fino a poco tempo anche alle macchine professionali con il problema che un'immagine, se zoomata, permette di cogliere anche particolari inquietanti (dai brufoli alle targhe delle auto anche se in lontananza).

Altra questione riguarda gli automatismi che hanno fatto dimenticare ai più le regole base di una bella fotografia, cogliere l'attimo o inviare un messaggio.

Di seguito sono riportate degli esempi di ripresa per far comprendere meglio le dinamiche di scatto di una foto rispetto agli obiettivi sia istituzionali che di protezione dei dati personali.

Da notare che è opinione di chi scrive, al di là dei consensi più o meno espliciti che i genitori possono esprimere, che la pubblicazione delle foto dei più piccoli (<14 anni) andrebbe comunque evitata a meno delle accortezze che riportiamo di seguito per completezza; si riportano inoltre degli esempi di riconoscimento dei dati personali:

 Anche senza riportare il nome o altri identificativi, la foto è immediatamente un dato personale.	 In questo caso i volti sono sfocati ma riconoscibili solo in ambito ristretto. Solo con altri identificativi la foto è un dato personale.	 La sfocatura impedisce il riconoscimento dei soggetti e quindi la foto non è un dato personale.
 Risoluzione troppo bassa, soggetti non riconoscibili e quindi la foto non è un dato personale.	 Effettuato Crop: la foto non è un dato personale.	 Soggetto non riconoscibile e quindi la foto non è un dato personale (sono troppi i ragazzi non avvezzi allo studio…)

Allegato 4 – Azioni e condizioni di liceità / rischi / accortezze necessarie

Al fine di semplificare la vita scolastica "digitale", è di seguito riportata una tabella con la mappatura degli strumenti con il da farsi, al fine di poter effettuare trattamenti di dati personali in conformità al Regolamento:

AZIONI	CONDIZIONE DI LICEITÀ	RISCHI	ACCORTEZZE
Pubblicazione foto/video su sito web scolastico	Informativa + doppio consenso (GDPR+Diritto d'autore)	Complessa la gestione dei soggetti senza consenso. Esposizione rispetto a sanzioni e cause risarcitorie.	Quelle riportate nella tabella precedente rispetto alla finalità della foto. Aggiungere nota degli obiettivi didattico- formativi rispetto alla possibilità di ripresa audio/video e foto nel PTOF
Pubblicazione foto/video su Social network istituzionale	Informativa + doppio consenso (GDPR+Diritto d'autore)	Il contratto previsto con il social network obbliga il rilascio di tutti i diritti. Impossibilità di attuazione dei diritti degli interessati	Evitare la riconoscibilità dei soggetti
Google Classroom istituzionale	Informativa + consenso (GDPR) per il solo utilizzo dei dati personali e di accesso	Rischi bassi a patto che non sia utilizzata come deposito di documenti contenenti dati sensibili	Regolamento sull'utilizzo degli strumenti, formazione in tema di sicurezza. Le policy Google prevedono la possibilità di gestione del consenso on-line solo ai maggiori di 14 anni. La questione è in evoluzione anche da parte di Google.
Cloud Drive (Google, Microsoft, ecc.) istituzionale	Informativa + consenso (GDPR) per il solo utilizzo dei dati personali e di accesso	Rischi bassi a patto che non sia utilizzata come deposito di documenti contenenti dati sensibili e che non avvengano indebite condivisioni	Regolamento sull'utilizzo degli strumenti, formazione in tema di sicurezza
Qualsiasi azione effettuata da un docente di istituto senza autorizzazione e con finalità personali	Non esistente la Condizione di liceità	Problemi reputazionali e di immagine	Regolamento sull'utilizzo degli strumenti, formazione in tema di sicurezza

Ripresa recita scolastica da parte dei genitori	Ambito ristretto, non necessaria la condizione di liceità	Pubblicazione sui social da parte di insegnanti o genitori	Vietare pubblicazione senza consenso delle immagini e delle riprese. Avvertire i genitori della necessità di condividere ad ambito ristretto le immagini e le riprese
Foto e riprese gita scolastica	Ambito ristretto, non necessaria la condizione di liceità	Pubblicazione sui social da parte di insegnanti o genitori	Vietare pubblicazione senza consenso delle immagini e delle riprese. Avvertire i genitori della necessità di condividere ad ambito ristretto le immagini e le riprese
Salvataggio documenti contenenti dati sensibili in dispositivi personali (es. computer di casa o USB drive)	Non presente, poiché non sono previste tutele e comportamento non regolamentato né posto in sicurezza	Data breach	Definizione di perimetro, Regolamento sull'utilizzo degli strumenti, formazione in tema di sicurezza, pseudonimizzazione, repository istituzionali
Pubblicazione elenchi allievi sul sito web istituzionale	Non esistente la Condizione di liceità	Diffusione di informazioni, soprattutto di categorie vulnerabili	Pubblicare solamente in piattaforme ad accesso ristretto con autenticazione, oppure pseudonimizzare con dati non direttamente riconducibili ai soggetti
Pubblicazione elenchi del personale supplente sul sito web istituzionale	Informativa e consenso	Diffusione di informazioni non previste dalle norme	Verificare che l'esportazione avvenga attraverso la specifica funzione denominata "privacy" e che siano riportati solamente i dati personali effettivamente necessari (nominativo, data nascita, provincia di nascita)
Pubblicazione prospetto assegnazione bonus docente	Norme sulla trasparenza	Diffusione di informazioni non previste dalle norme	Le pubbliche amministrazioni pubblicano i dati relativi all'ammontare complessivo dei premi collegati alla performance stanziati e l'ammontare dei premi effettivamente distribuiti" e pubblicano i criteri definiti nei sistemi di misurazione e valutazione della performance per l'assegnazione del trattamento accessorio e i dati relativi alla sua distribuzione, in forma aggregata, al fine di dare conto del livello di selettività utilizzato nella distribuzione dei premi e degli incentivi, nonché i dati relativi al grado di differenziazione nell'utilizzo della premialità sia per i dirigenti sia per i dipendenti

Allegato 5 – Commento alle piattaforme gratuite come di Google

"Chi ha paura del digitale?"

Il DPO/RPD ha per vocazione una certa sensibilità al tema della protezione dei dati personali; lo si deve sia alla missione che ci avete affidato, sia alle spiacevoli situazioni che abbiamo dovuto gestire e risolvere.
Spesso quando *i buoi erano già scappati*.

La scuola dovrebbe essere un faro che illumina la strada dei ragazzi e li protegge dai rischi connessi con l'uso indiscriminato delle nuove tecnologie, e dei social. Ma spesso i modelli di riferimento dei ragazzi non sono adeguatamente formati. Anzi, l'esperienza insegna che sono i primi a fare un uso non attento, superficiale oppure sconsiderato di questi strumenti.

Senza regole né gestori, nel *selvaggio mondo digitale,* rischiamo di apparire come gli ultimi *pasdaran* della normativa sui dati personali; in realtà non si tratta di essere integralisti o meno, ma troppo spesso rileviamo approcci strumento-centrici imperniati più sulle funzionalità, sulla semplicità, sulla gratuità che non sulla tutela dei dati o sui loro potenziali rischi presenti e futuri.

Le possibilità che il digitale regala a tutti noi in termini di velocità, comodità ed economicità è, intendiamoci, un po' come la mela di Biancaneve: un oggetto fantastico gravato da una pesante ipoteca.

Per prima cosa, teniamo sempre a mente che le informazioni su di noi valgono oro. Da quanto abbiamo visto con i casi *Facebook-Cambridge Analytica* o *Google-Mastercard*, ci sono in ballo affari miliardari che sfuggono alla nostra comprensione.

Poi, c'è anche il fatto che non possiamo sapere oggi cosa succederà domani con tutta la mole di dati che giorno per giorno, come *side effect*, regaliamo alle varie piattaforme social o didattiche che siano. È vero che nel contratto con Google si parla di *minima ingerenza* e di *nessuna pubblicità* ma non si può escludere la possibilità che gli iscritti vengano profilati. Se non ora, in futuro.

Ma la profilazione sarebbe tutto sommato un aspetto trascurabile se riguardasse solo la creazione di un identikit per definire, per quanto in modo specifico, il soggetto destinatario di promozioni commerciali. La profilazione è, invece un pericolo quando la raccolta di informazioni nasconde la volontà di un vero e proprio *dossieraggio a* scopi politici, oppure quando integra la possibilità di ricostruire la storia genetico- sanitaria del soggetto ad uso e consumo delle società assicurative che andranno a valutare i rischi della loro attività...

Con Google c'è, poi, un altro problema da affrontare: dove vanno a finire i nostri dati? La risposta è semplice: su data center esterni, posizionati al di fuori dell'Unione Europea, dove vigono regole (o *non regole*) diverse inserite in sistemi giuridici che non appartengono alla nostra cultura e che, spesso non condividono la nostra stessa scala di valori.

Salvare "capra e cavoli" si può?

Noi che tanto tempo fa abbiamo iniziato a vivere l'informatica, non possiamo che apprezzare l'intento pedagogico di un progetto di implementazione di piattaforme digitali che promuova e incoraggi il lavoro collaborativo online e lo sviluppo di competenze sociali, organizzative e digitali.

Adottare la cosiddetta G Suite in ambiente didattico comporta aspetti che richiedono competenze tecniche e giuridiche non alla portata di tutti. Il documento che segue si pone l'obiettivo di trovare una soluzione che tuteli le nuove generazioni dai rischi connessi alle tecnologie dell'informazione, ma che non impedisca, al contempo, l'utilizzo della piattaforma.

La prima cosa da notare riguarda l'account simil filantropico <nomeallievo>@<nomescuola>.it, che alla fine del ciclo scolastico sarà di sicuro convertito in account <nome>@gmail.com, di tipo *consumer*, e, pertanto, al di là di quanto dichiarato nelle articolate e complesse informative di Google sulla tutela dei dati personali, sarà utilizzato esclusivamente per scopi commerciali.

Altra questione riguarda la professione docente: sembra che, per visione ministeriale e del singolo insegnante innamorato o costretto "digitale", la *materia educativa* ruoti attorno alla piattaforma G Suite.

D'accordo sul fatto che il MIUR avrebbe potuto investire in una piattaforma tutta italiana, dove poter condividere i lavori fatti tra colleghi; siamo anche consci, però, che le istituzioni scolastiche non possono permettersi un servizio di questo tipo, tantomeno personale in grado di gestire infrastrutture complesse.

Inoltre, le nuove generazioni hanno abbassato notevolmente il tempo massimo di attenzione prima della *disattivazione cerebrale* e sarebbe preferibile lavorare a monte sulle *soft skill* e sulle tecniche di presentazione, comunicazione, relazione interpersonale, piuttosto che sulle fredde piattaforme digitali.

Per questi motivi, la cosa migliore è adottare un sano principio di precauzione, attivando tutte le possibili cautele per proteggere i nostri dati e quelli degli allievi. E le famiglie dovrebbero essere adeguatamente informate per scegliere liberamente, senza vincoli o costrizioni, avendo più opzioni disponibili.

Svoltando sulle formalità di applicazione normativa, nel caso che si decida di procedere all'implementazione della piattaforma, è necessario informare i genitori e richiedere loro il consenso; per questo motivo abbiamo integrato l'informativa standard prevista da Google con ulteriori informazioni, che forniamo a richiesta.

L'eventuale mancata autorizzazione da parte delle famiglie non impedisce a priori l'introduzione della piattaforma G Suite in classe; un piccolo *escamotage*, anche carino in ambito scolastico, è l'utilizzo dei cosiddetti *nickname* o soprannomi, magari del mondo dei fumetti o dei film *fantasy*.

Sarà cura dell'insegnante gestire di volta in volta la conversione tra nome (vero) e *nickname*, evitando di salvare la lista ovviamente sul drive condiviso.

Infine, consigliamo l'adozione di un regolamento o la distribuzione di istruzioni dettagliate sull'uso delle piattaforme on-line e più in generale di tutti gli strumenti cloud che dovessero diventare più o meno "ufficiali" nella singola istituzione scolastica. In questo modo, insegnati e studenti potranno beneficiare delle potenzialità di questi strumenti, in modo consapevole, riducendo al minimo i rischi connessi.

Se avete dubbi o domande, necessità di approfondimenti, potete scrivere a dpo@morolabs.it.

La versione slide animate del presente documento è disponibile all'indirizzo:

https://www.icgigli.edu.it/gdpr-e-privacy/