

STUDIO LEGALE
Avv. Emanuela Caricati
Piazza Santo Stefano n. 14 – 15121 Alessandria (AL)
Via Medaglie D'Oro Sinisi n. 43 – 75025 Policoro (MT)
Tel 3920192041

Policoro, lì 30 marzo 2020

Alla c.a. del Dirigente Scolastico
e, p.c. del DSGA

Oggetto: Provvedimenti e indicazioni Garante Privacy sulla didattica a distanza.

Gentili,

con la presente si provvede ad analizzare i provvedimenti e le prime indicazioni fornite Dal Garante Privacy in merito al trattamento dei dati personali degli interessati, relativamente alle attività connesse alla didattica a distanza (DaD).

Come già affermato nella nostra comunicazione del 9 marzo u.s., la scuola non deve richiedere alcun consenso agli interessati per lo svolgimento della didattica a distanza.

L' Autorità sul punto ha affermato che *“Le scuole e le università sono autorizzate a trattare i dati, anche relativi a categorie particolari, di insegnanti, alunni (anche minorenni), genitori e studenti, funzionali all'attività didattica e formativa in ambito scolastico, professionale, superiore o universitario [...]. In tal senso dispone la normativa di settore [...] per tutta la durata della sospensione delle attività didattiche in presenza nelle scuole, nelle università e nelle istituzioni di alta formazione [...]. Non deve pertanto essere richiesto agli interessati (docenti, alunni, studenti, genitori) uno specifico consenso al trattamento dei propri dati personali funzionali allo svolgimento dell'attività didattica a distanza, in quanto riconducibile – nonostante tali modalità innovative – alle funzioni istituzionalmente assegnate a scuole ed atenei”.*

Come già anticipato nella nostra comunicazione del 9 marzo u.s., le istituzioni scolastiche non devono procedere alla valutazione d'impatto però, nella scelta della piattaforma, in ossequio al principio di privacy by design, occorrerà individuare quella maggiormente rispondente ai principi di liceità e minimizzazione del trattamento, con particolare riferimento alle tecniche di monitoraggio dell'attenzione o di profilazione.

L' Autorità, infatti, ha specificato che *“La valutazione di impatto, che l'art. 35 del Regolamento richiede per i casi di rischi elevati, non è necessaria se il trattamento effettuato dalle istituzioni scolastiche e universitarie, ancorché relativo a soggetti in condizioni peculiari quali minorenni e lavoratori, non presenta ulteriori caratteristiche suscettibili di aggravarne i rischi per i diritti e le libertà degli interessati. Ad esempio, non è richiesta la valutazione di impatto per il trattamento effettuato da una singola scuola (non, quindi, su larga scala) nell'ambito dell'utilizzo di un servizio on line di videoconferenza o di una piattaforma che non consente il monitoraggio sistematico degli utenti o comunque non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici).”*

Per quanto riguarda la nomina del Responsabile esterno, sempre come già anticipato nella nostra nota del 9 marzo u.s., l'adempimento è ovviamente da intendersi assolto nel caso del registro elettronico.

Non è prevista alcuna nomina, invece, nel caso di utilizzo di piattaforme terze per la DaD. Infatti, il Garante della Privacy, nel provvedimento allegato, ha stabilito che *“[...] Qualora il registro elettronico non consentisse videolezioni o altre forme di interazione tra i docenti e gli studenti, potrebbe essere sufficiente – per non dover designare ulteriori responsabili del trattamento- utilizzare servizi on line accessibili al pubblico e forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato. Alcuni di questi servizi sono, peraltro, facilmente utilizzabili anche senza la necessaria creazione di un account da parte degli utenti “*

Vi comunichiamo, inoltre, le seguenti procedure da attivare/verificare per garantire la conformità al GDPR delle attività connesse alla DaD.

- Fate in modo che le applicazioni per la videoconferenza siano gestite in un **ambiente riservato** (ad esempio Meet tramite il dominio riservato G Suite), evitando applicazioni per la videoconferenza che mettono a disposizione stanze “**pubbliche**” per le attività. Tanto si rende necessario per garantire che i partecipanti alle attività siano **solo ed esclusivamente gli aventi diritto** ed evitare la presenza di utenze estranee e non autorizzate.
In alternativa si rende necessario (laddove possibile) proteggere l’accesso al meeting tramite un codice riservato o altra procedura similare.
In ogni caso, deve sempre essere possibile **identificare la presenza** di utenze esterne e non approvate, durante un meeting e più in generale durante qualunque attività riferita alla DaD.
- Accertarsi che gli strumenti individuati per la DaD e specificatamente quelli per le videoconferenze **non adottino sistemi di monitoraggio sistematico degli utenti**. In tal caso è necessario disattivare tale opzione.
- Accertarsi che gli strumenti individuati per la DaD non facciano ricorso alla **geolocalizzazione** o a **sistemi di social login** (accesso alla piattaforma basato, ad esempio, su un account Facebook persistente). Più in generale è necessario verificare che gli strumenti adottati per la DaD non adottino **tecniche di profilazione¹ dei dati a fini commerciali**.
- Attenzione alle procedure messe a disposizione dagli strumenti per la videoconferenza relative alla **registrazione del meeting**. Tale registrazione (sia da parte dei docenti che degli allievi) è da considerarsi legittima se **utilizzata a scopi esclusivamente personali²**. È esclusa qualsiasi forma di diffusione o comunicazione senza il consenso esplicito di tutti gli interessati. Ovviamente, la responsabilità della comunicazione o della diffusione è direttamente relazionata al singolo individuo. Anche la disabilitazione (ove possibile) di tale funzione non risolve alla radice il problema: sarebbe, comunque, possibile e banalmente con altri strumenti registrare il meeting (così come sarebbe possibile durante l’attività in presenza). La soluzione è da ricercarsi nel livello di consapevolezza e responsabilità dell’utenza.

Alleghiamo il Provvedimento del Garante della Privacy.

Rimaniamo a Vostra disposizione.

Cordialità

Emanuela Caricati

Francesco Sandro Della Rocca

¹ Normalmente, con l’espressione profilazione per finalità commerciali o di marketing, ci si riferisce all’analisi e all’elaborazione di informazioni relative agli utenti di un determinato servizio on line finalizzata alla creazione di gruppi omogenei per gusti e comportamenti (profili) funzionali a pervenire all’identificazione del singolo utente, o più spesso di un gruppo di utenti, o del terminale da cui si collega, al fine di proporre offerte personalizzate di beni o servizi ulteriori o affini.

² Cfr. “La Privacy a Scuola – Le regole da ricordare” – Garante delle Privacy.