Prof. Dott. Giuseppe Chiumeo
DPO RPD – Data Protection Officer – Responsabile Protezione Dati
Docente di informatica
IT Specialist and Consultant
Vicario del Dirigente Scolastico c/o ITET "Cassandro Fermi Nervi"
Docente incaricato presso la Facoltà Teologica Pugliese
IT Security Expert - Esperto in Sicurezza Informatica
Esaminatore e supervisore ICDL
Webmaster

Alla c.a. del
Dirigente Scolastico
Titolare del trattamento dati

e, p.c. Alla c.a. del/dei
Responsabile/i del trattamento dati

Barletta, 25/04/2022

Oggetto: Privacy, avvertenze per la conclusione dell'anno scolastico ed adempimenti generici. Comunicazione n° 6.

Gent.mo Dirigente Scolastico,
in virtù dell'imminente conclusione dell'anno scolastico, mi preme ricordare e rispolverare, in qualità di DPO - Responsabile della Protezione dei Dati, alcuni aspetti in tema di privacy di notevole delicatezza da osservare ed inerenti i seguenti argomenti:

- Fascicolo del personale scolastico;
- Utilizzo corretto del Registro elettronico di classe;
- Maturità: il "documento del 15 maggio" e le indicazioni del Garante della Privacy;
- Implementazione corretta di un sito web scolastico.

Inoltre, nell'ultima parte della presente, a seguito di numerosi quesiti pervenuti allo scrivente da parte delle istituzioni scolastiche durante l'anno in corso, riporto alcune tematiche di particolare interesse e sempre d'attualità:

- Videosorveglianza a scuola;
- Buone pratiche per la cyber-security nelle scuole.

Fascicolo del personale scolastico

Come sappiamo, i fascicoli dei dipendenti scolastici contenenti l'intera documentazione relativa a ciascun soggetto, aggiornata di anno in anno e di servizio in servizio, che siano cartacei o digitali, seguono il lavoratore anche in caso di passaggio da una scuola all'altra. Il fascicolo deve perciò accompagnare l'interessato e, in caso di trasferimento o assegnazione definitiva di sede, va trasmesso al nuovo istituto che ne deterrà la titolarità. Ogni scuola deve infatti essere depositaria dei soli fascicoli dei dipendenti in servizio, e non di quelli che vi hanno lavorato in passato.

Le norme generali previste dagli art.24 e ss. del D.P.R. 686/1957 impongono che nella documentazione che caratterizza il fascicolo del personale scolastico rientrino diverse tipologie di dati raccolti, tra cui:

- I dati anagrafici e fiscali, così come le coordinate utili all'accredito degli emolumenti previsti per il dipendente;
- I titoli di studio, i titoli professionali e gli attestati di formazione e aggiornamento;
- I contratti di lavoro, sia a tempo determinato che indeterminato, stipulati con l'istituzione scolastica;
- La documentazione relativa al passaggio di ruolo, così come all'assegnazione di sede definitiva;
- Gli atti inerenti il periodo di prova, così come il decreto di conferma in ruolo, e tutte le richieste di ricostruzione di carriera;
- La documentazione inerente le assenze del dipendente: malattia, congedi, permessi previsti dalla legge e dai CCNL, astensione per maternità;
- La documentazione inerente eventuali procedimenti disciplinari;
- Lo stato matricolare;
- Gli atti inerenti mobilità, comandi, esoneri, distacchi sindacali, ecc.;
- Gli incarichi ottenuti dall'istituzione scolastica;
- La documentazione relativa al collocamento a riposo, quali richieste e pratiche di TFS e TFR, ad esempio.

I fascicoli "personale scolastico" vanno così conservati seguendo specifiche modalità, al fine di tutelare la riservatezza delle informazioni contenute all'interno degli stessi, evitando il trattamento dei dati qualora non rientri nelle ragioni d'ufficio o da parte di soggetti non autorizzati e nel rispetto delle norme previste in materia. Ogni scuola è perciò tenuta ad adottare un vero e proprio manuale di gestione documentale, entro cui specificare quali possono essere i soggetti autorizzati al trattamento della documentazione contenuta all'interno dei fascicoli, ponendo come specifica le mansioni e le responsabilità da parte di ciascun operatore.

Viene da sé che, qualora necessario, l'istituto potrà richiedere alle altre scuole – anche al di fuori della provincia o della regione – l'invio di tutti gli atti che permettono di emanare eventuali provvedimenti di propria competenza. Il fascicolo dovrà essere trasmesso tramite lettera di accompagnamento, integrata da un elenco dettagliato legato alla documentazione presente, di cui la scuola mittente dovrà conservare copia sul proprio sistema di protocollo. In presenza di atti e documenti riservati, quali ad esempio i procedimenti disciplinari, è preferibile l'invio in busta chiusa accompagnata da indicazione "documenti riservati", da sottoporre all'attenzione del dirigente scolastico dell'istituto di destinazione.

Grazie al lavoro congiunto tra Ministero dell'Istruzione, Ministero della Cultura, AgID e Istituzioni scolastiche sono stati predisposti e/o aggiornati gli strumenti volti a supportare le segreterie scolastiche nel processo di gestione dei flussi documentali digitali (cd gestione documentale).

Si ricorda che ciascun dipendente scolastico ha il diritto di visionare ed estrarre copia della documentazione raccolta all'interno del proprio fascicolo personale nel rispetto della normativa generale sul diritto di accesso agli atti previsto dagli art.22 e ss della L. 241/90. Tale diritto risulta esercitabile fino al momento in cui la pubblica amministrazione presenta l'obbligo di detenere e conservare i documenti amministrativi per i quali si richiede l'accesso. Non sarà possibile dunque avere accesso agli atti ove la scuola abbia trasmesso il fascicolo personale ad altro istituto, nel caso ad esempio in cui il dipendente sia stato trasferito.

Utilizzo corretto del registro elettronico

Il registro elettronico è ritenuto a tutti gli effetti un documento ufficiale, pertanto, modificarne i voti, rappresenta dunque un "falso ideologico".

Occorre dunque che i docenti prestino particolare attenzione nell'utilizzare questo strumento, registrando in tempo reale quanto si verifica in classe. Troppo spesso, da quando il registro elettronico è stato introdotto ufficialmente nelle scuole, i genitori hanno lamentato un uso scorretto dello stesso da parte dei docenti.

I motivi sono molteplici e spaziano dalle valutazioni assegnate con ritardo rispetto alle interrogazioni orali o alla correzione dei compiti scritti, alla compilazione del registro a fine giornata (o in taluni casi anche a distanza di una settimana), senza tralasciare i voti registrati e modificati in un secondo momento.

I docenti devono perciò essere consapevoli che registrare online un voto di una verifica, per poi modificarlo successivamente, è un'operazione digitale di cui resta traccia nei server.

Nel caso di un errore di trascrizione o digitazione, in virtù del fatto che ogni azione è tracciabile, ogni cambiamento andrà motivato tramite una relazione scritta firmata dallo stesso docente e posta all'attenzione non solo del dirigente scolastico, ma anche dei familiari dell'alunno (anche una nota sullo stesso registro elettronico per i familiari che giustifichi il cambio del voto potrebbe essere sufficiente).

Ciò al fine di evitare fraintendimenti, richiami o pesanti sanzioni disciplinari.

Maturità 2021: il "documento del 15 maggio" e le indicazioni del Garante della Privacy

Secondo quanto espresso dall'Ordinanza Ministeriale n.53 del 3 marzo 2021 relativa agli Esami di Stato del II ciclo, il consiglio di classe deve attenersi a un iter specifico, espresso nell'art. 10 della stessa, il quale afferma che: "entro il 15 maggio 2021 il consiglio di classe elabora, ai sensi dell'articolo 17, comma 1, del Dlgs 62/2017, un documento che esplicita i contenuti, i metodi, i mezzi, gli spazi e i tempi del percorso formativo, i criteri, gli strumenti di valutazione adottati e gli obiettivi raggiunti, nonché ogni altro elemento che lo stesso consiglio di classe ritenga utile e significativo ai fini dello svolgimento dell'esame".

Nella stesura di tale documento, chiamato comunemente "documento del 15 maggio", il consiglio di classe deve inoltre tenere conto delle indicazioni fornite dal Garante per la protezione dei dati personali attraverso la Nota del 21 marzo 2017, che ne esplica le modalità operative, al fine di tutelare gli studenti da una scorretta diffusione di dati personali nell'ambito della pubblicazione del suddetto.

In tale nota il Garante della Privacy sottolinea quanto sia importante che gli istituti scolastici, nello svolgimento delle proprie funzioni istituzionali, agiscano nel totale rispetto dei diritti e delle libertà fondamentali, nonché della dignità degli studenti, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali.

Secondo il quadro normativo sulla protezione dei dati personali, come sostiene lo stesso Garante, "*non è presente alcuna ragionevole evidenza della necessità di fornire alla commissione esaminatrice dati personali riferiti agli studenti in un documento volto principalmente ad orientare tale commissione nella preparazione dell'esame*", in particolare a fronte delle novità introdotte mediante l'Ordinanza Ministeriale 205/2019.

Viene da sé che il ruolo del cosiddetto "documento del 15 maggio" è quello di evidenziare il percorso didattico e formativo di ciascuna classe, prescindendo dalle peculiarità dei singoli studenti che la costituiscono: la diffusione dello stesso risulterebbe pertanto priva di un necessario fondamento normativo che possa in qualche modo giustificare tale azione.

Tuttavia al documento possono essere altresì allegati atti e certificazioni relativi alle prove effettuate e alle iniziative realizzate durante l'anno in preparazione dell'Esame di Stato, ai Percorsi per le Competenze Traversali e per l'Orientamento o PCTO, agli stage e ai tirocini eventualmente effettuati, alle attività e progetti svolti nell'ambito del previgente insegnamento di Cittadinanza e Costituzione e dell'insegnamento dell'Educazione Civica riferito all'anno scolastico 2020/21.

Lo stesso documento dovrà poi essere opportunamente pubblicato nell'albo online della scuola: proprio per questo non deve in alcun modo contenere dati personali relativi agli studenti.

Come indicato anche nel vademecum "La scuola a prova di privacy" fornito dal Garante per la protezione dei dati personali, gli esiti degli scrutini e degli Esami di Stato sono pubblici. Le informazioni sul rendimento scolastico di ciascuno studente sono infatti sottoposte a un regime di conoscibilità definito dal Ministero dell'Istruzione. Tuttavia rappresenta una condizione necessaria e imprescindibile che, nel pubblicare gli esiti degli scrutini e degli esami apposti sui tabelloni, l'istituto scolastico eviti di fornire, seppur indirettamente, informazioni relative allo stato di salute degli studenti o qualsivoglia dato personale non pertinente.

Un esempio è rappresentato dalle "prove differenziate" sostenute dagli studenti diversamente abili (DVA) o con disturbi legati all'apprendimento (DSA), le cui problematiche non possono essere rese di dominio pubblico ma semplicemente indicate nell'attestazione rilasciata agli stessi.

Per quanto concerne invece la possibilità di fotografare i tabelloni scolastici, il Garante della privacy ha sottolineato che "nessuna norma del Codice sulla protezione dei dati personali preclude la piena pubblicità degli scrutini scolastici, la possibilità di accesso ai luoghi dove essi sono esposti e di trarne notizia prendendo appunti per usi personali, eventualmente anche con foto. Non si può utilizzare il Codice per precludere la piena pubblicità degli esiti finali: se poi vi fosse, a posteriori, un eventuale uso non corretto, questo sarebbe ovviamente verificabile. Inoltre, i dati relativi agli esiti scolastici, per quanto riferiti a minori, non sono dati sensibili, non riguardano cioè informazioni sullo stato di salute, le opinioni politiche, le appartenenze religiose, l´etnia o gli stili di vita, ma attengono esclusivamente al rendimento scolastico degli allievi".

L'importanza per la scuola di un sito web "a prova di privacy"

Oggi tutte le scuole sono dotate di un sito internet con cui rendono partecipi i visitatori esterni – e in particolare le famiglie e gli studenti – delle attività svolte e dei progetti realizzati. Il portale istituzionale viene poi utilizzato anche per adempiere agli obblighi normativi di pubblicità e trasparenza, in modo da notificare al pubblico l'operato della scuola.

Per queste ragioni, ciascun istituto deve essere consapevole del fatto che il proprio sito va allineato al GDPR, normativa che disciplina la protezione dei dati personali da ormai quasi quattro anni.

Le pubbliche amministrazioni devono adeguarsi al Regolamento Europeo, ponendo al centro la protezione dei dati, al fine di evitare il rischio di incorrere in sanzioni piuttosto salate. È importante perciò non farsi cogliere impreparati, sia sotto l'aspetto funzionale ed estetico, ma ancor di più sotto quello normativo.

Cosa fare dunque per creare un sito web "a prova di privacy"? Ecco i principali step da compiere.

- La prima regola per rendere sicuro un portale web prevede che lo stesso sia in grado di trasmettere le informazioni mediante protocollo "https", evitando quindi l'ormai obsoleto "http". A fare la differenza in questo caso è la "S", che significa "secure". A livello di percezione, un sito che mostra l'indicazione "non sicuro" nella barra degli indirizzi è quanto di peggio si possa rintracciare navigando in rete. Non si tratta solamente di una banale criticità che coinvolge l'immagine del portale, ma anche e soprattutto della sicurezza nella trasmissione delle informazioni e dei dati personali. Applicare il protocollo "https" significa che i contenuti presenti all'interno del sito sono criptati, e quindi protetti dagli attacchi hacker, specie se il sito, come dovrebbe essere oggigiorno, preveda la profilatura dei docenti in servizio con alcuni dati personali e password. Per realizzare tale migrazione verso l'https, è necessario acquistare un certificato SSL – per poi mantenerne la validità effettuando i dovuti aggiornamenti – ed anche questo fornisce un'immagine di serietà, tutelando i dati personali degli utenti, ed evitando di conseguenza che il Garante della Privacy intervenga con sanzioni per violazione della normativa.
- Ogni sito deve essere sottoposto a un'analisi tecnica da parte del webmaster, al fine di definire quali tipologie di cookie siano effettivamente presenti. Da tale report dipenderanno le decisioni dell'amministratore dello spazio web, che dovrà adeguare la "cookie policy" alla normativa, applicando i banner necessari. Il tutto secondo le indicazioni contenute nelle "Linee guida in materia di Cookie e altri strumenti di tracciamento" del Garante per la Protezione dei Dati Personali (provvedimento n. 231 del 10 giugno 2021), obbligatorie dal 9 gennaio 2022.
- Anche l'informativa privacy del sito deve necessariamente indicare in maniera specifica quali sono i dati trattati. Non solo dunque quelli legati alla navigazione, ma anche quelli forniti dagli utenti in maniera volontaria, qualora siano presenti moduli di contatto o newsletter. La policy deve poi rispondere in maniera efficace a tutti i requisiti previsti dagli artt. 12 e 13 del GDPR. Una buona pratica è sicuramente quella di rendere disponibile l'informativa del sito tramite un link posto nel

footer della pagina. È infatti preferibile che l'informativa sia consultabile da ogni sezione del sito, e non solo dall'homepage. Inoltre, per un più efficiente adempimento dell'obbligo di intelligibilità dell'informativa, è opportuno fare precedere o seguire i diversi punti di raccolta di dati personali/moduli da un'informativa contenente le informazioni direttamente riferibili a quella specifica raccolta. Pertanto, con particolare riferimento al modulo utilizzato per ricevere la MAD (operazione che si attiva solitamente subito dopo la conclusione dell'anno scolastico), la scuola è tenuta a predisporre l'apposita informativa correlata alla finalità specifica. Mi permetto, quando si parla di sicurezza riferita a un sito web, di sottolineare di come il detto "chi più spende, meno spende" sia assolutamente pertinente nella costruzione di un sito che garantisca un alto livello di sicurezza. Non è infatti una regola che il servizio più economico sia quello più conveniente, e non solo per fattori quali la competenza e la professionalità. I fornitori del "web hosting" devono infatti essere "compliant" al GDPR, informando preventivamente il titolare del sito sulla locazione del server e su altri aspetti. Vanno inoltre nominati "responsabili esterni del trattamento", in quanto i dati che transitano sul sito vengono visualizzati anche da terzi, ed è perciò fondamentale definire i ruoli per essere certi di ottemperare al principio di accountability che determina le responsabilità del titolare rispetto alle informazioni raccolte.

Videosorveglianza a scuola

Come già noto, secondo quanto stabilito dal Garante, gli istituti scolastici possono installare e utilizzare videocamere di sorveglianza (purché in grado di garantire il diritto alla riservatezza di ogni studente) nel caso in cui ciò risulti indispensabile al fine di tutelare l'edificio e i beni in esso contenuti da atti vandalici e furti, circoscrivendo tuttavia le riprese alle sole aree interessate.

L'installazione dell'impianto di videosorveglianza da parte della scuola, appare pertanto lecita solo se avvalorata da una concreta esigenza di prevenire situazioni di pericolo sorte a seguito di episodi di furto o atti vandalici già verificatisi o, in alternativa, nel caso in cui la scuola custodisca beni di valore quali strumentazione informatica o somme di denaro.

Le riprese devono tuttavia risultare circoscritte alle sole aree interessate da furti o atti vandalici, e la presenza delle telecamere deve essere al contempo opportunamente e chiaramente segnalata da un'apposita cartellonistica. Secondo quanto stabilito dal Garante della Privacy, le aree esterne adiacenti all'istituto scolastico possono essere oggetto di riprese mediante telecamere di videosorveglianza anche durante le lezioni, purché non risultino pertinenti all'edificio. Al contrario, le aree interne della scuola possono essere oggetto di riprese solo ed esclusivamente negli orari di chiusura, e non dunque durante l'ordinario svolgimento delle attività scolastiche o extrascolastiche.

Il Garante appare particolarmente attento nella gestione dei sistemi di videosorveglianza: questo poiché uno scorretto utilizzo delle telecamere può comportare un'ingerenza ingiustificata nella vita del soggetto, con conseguente violazione dei diritti e delle libertà fondamentali.

Importante è l'informativa in merito alle riprese: essa in questo caso può essere rappresentata da un modello semplificato, o in alternativa da un semplice cartello, che tuttavia deve contenere, tra le altre informazioni, le indicazioni sul titolare del trattamento e sulla finalità perseguita. Il modello può essere adattato a specifiche circostanze o contesti quali la presenza di più telecamere, la vastità dell'area oggetto di rilevamento o le modalità delle riprese, e l'informativa deve essere collocata in maniera visibile in prossimità o nelle immediate vicinanze della zona sorvegliata. Non è necessario rivelare la precisa ubicazione della telecamera, purché non vi siano dubbi su quali zone siano soggette a sorveglianza e sia chiarito in modo inequivocabile il contesto della sorveglianza stessa. L'interessato deve poter comprendere in modo chiaro quale zona sia coperta dalla telecamera a scuola, in modo da evitare la sorveglianza o adeguare il proprio comportamento, ove necessario. L'informativa deve rinviare a un testo completo contenente tutti gli elementi di cui all'art. 13 del GDPR, indicando come e dove trovarlo (ad esempio sul sito internet del titolare del trattamento, o affisso in bacheche o locali dello stesso).

Infine è necessario che il titolare del trattamento dei dati personali nomini per iscritto tutti i soggetti che in suo nome e conto abbiano facoltà di trattare le immagini (ritenute al pari dei dati personali) raccolte mediante impianti di videosorveglianza a scuola. Essi non sono altro che soggetti interni alla scuola che hanno accesso alle immagini e ai locali dove sono situate le postazioni di controllo o, in alternativa, i responsabili del trattamento che, secondo quanto stabilito dall'art. 28 del GDPR, sono quei soggetti esterni che hanno accesso alle immagini, quali ad esempio le società che si occupano dell'impianto di videosorveglianza e della relativa manutenzione. A tal proposito si allegano modelli di nomine sia per personale interno che esterno compilabili e personalizzabili.

Buone pratiche per la cybersecurity nelle scuole

Ai sensi dell'art. 32 del GDPR, la scuola, in qualità di soggetto titolare del trattamento, "tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche", deve implementare e mettere in atto misure tecniche e organizzative tali da garantire un livello di sicurezza adeguato al rischio.

Detto più semplicemente, il titolare ha il dovere di accertarsi che le informazioni personali degli interessati siano protette in ogni circostanza. Le misure di sicurezza da adottare devono essere finalizzate a ridurre al minimo i rischi di distruzione o perdita dei dati, accesso non autorizzato, trattamento non consentito e modifica degli stessi.

Il Garante, con provvedimento del 2 luglio 2015, ha definito quali siano le "Misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche", e nello specifico ha affermato – al punto 5, lettera e) dell'allegato B – che "nel caso le credenziali siano costituite da una coppia username/password, siano adottate le seguenti politiche di gestione delle password:

- la password, comunicata direttamente al singolo incaricato separatamente rispetto al codice per l'identificazione (user id), sia modificata dallo stesso al primo utilizzo e, successivamente, almeno ogni tre mesi, e le ultime tre password non possano essere riutilizzate;
- le password devono rispondere a requisiti di complessità (almeno otto caratteri, uso di caratteri alfanumerici, lettere maiuscole e minuscole, caratteri estesi);
- le credenziali di ciascun dipendente devono essere conservate in busta sigillata e sottoscritta in cassaforte: in caso di mancanza o assenza del dipendente e a fronte della necessità di dover accedere per emergenza al profilo digitale del dipendente per il recupero di alcuni file importanti allora si potrà procedere nell'apertura della busta sigillata previa verbalizzazione dell'operazione da parte del titolare del trattamento (DS); la password, al rientro del dipendente, sarà prontamente cambiata e conservata secondo la modalità descritta;
- quando l'utente si allontana dal terminale, la sessione deve essere bloccata, anche attraverso eventuali meccanismi di time-out;
- le credenziali devono essere bloccate a fronte di reiterati tentativi falliti di autenticazione.

Oltre a ciò, dobbiamo aggiungere che il continuo sviluppo tecnologico determina un costante aggiornamento dei sistemi di protezione da adottare. Oggi, ad esempio, è consigliabile utilizzare sistemi di autenticazione a due fattori, volti a garantire una maggiore sicurezza dei dati conservati all'interno delle piattaforme.

Fondamentale è dunque che i dirigenti e il personale della scuola siano consapevoli dei rischi a cui possono andare incontro se non vengono adottate politiche di controllo degli accessi logici ai dati trattati attraverso sistemi informatici, secondo ruoli e responsabilità definite e profili personali attribuiti agli utenti.

Quindi – se la scuola non l'ha già fatto – il consiglio è quello di creare per ciascun utente specifici account di accesso ai programmi, evitando che più persone operino con un unico account sugli applicativi dell'istituto.

Restando a disposizione per ogni eventuale chiarimento in merito, colgo l'occasione per salutarla cordialmente suggerendo anche la frequente consultazione del sito del garante della privacy (garanteprivacy.it e gdprscuola.it).

Prof. Giuseppe Chiumeo
Responsabile della protezione dei dati della scuola