

<p>POLICY</p> <p>CLASSIFICAZIONE DELLE INFORMAZIONI</p> <p>COD. C.18</p> <p>VERSIONE N. 01 DEL 08.2022</p>

CONTIENE:

- 1. POLICY

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE



PREMESSA

Il processo di classificazione dei dati in due o più categorie aiuta il personale a comprendere e distinguere i limiti entro i quali una determinata informazione può essere condivisa con uno o più soggetti. Nel corso della vita di una scuola, difatti, non è sempre agevole comprendere velocemente se una informazione può essere inviata o meno ad un soggetto, sia esso interno o esterno all'organico scolastico. La classificazione dei dati, e la loro conseguente etichettatura, viene in soccorso proprio al fine di evitare fraintendimenti e incertezze all'origine della maggior parte dei casi di data breach. Non a caso, l'obiettivo della sicurezza delle informazioni è solitamente legato alla protezione di Riservatezza, Integrità e Disponibilità (RID) dei dati. La classificazione dei dati riflette il livello di rischio che la scuola deve sopportare se la riservatezza, l'integrità o la disponibilità sono compromesse da una violazione di dati che può avvenire sia da parte di soggetti esterni (per dolo) sia da soggetti interni (per colpa) all'organizzazione stessa.

CRITERI

Il rischio di violazione è tuttavia diverso in base al bene che si vuole tutelare. Parlando di scuole, potremmo prendere in considerazione due tipologie di classificazioni (non concorrenti tra loro) e in particolare: quella richiesta da AGID e quella richiesta in base al GDPR.

La differenza consiste nel fatto che, mentre AGID classifica i dati in base all'impatto che un'eventuale diffusione avrebbe sulla sicurezza nazionale, a livello scolastico, sotto il punto di vista GDPR, potremmo classificare le informazioni in base alla loro riservatezza e, quindi, in base alla loro capacità di circolazione in base alla normativa europea. Come si diceva, queste due tipologie di classificazione non sono concorrenti, anzi, ogni scuola dovrebbe dapprima eseguire la classificazione richiesta da AGID e, successivamente, dovrebbe operare la classificazione di cui al GDPR.

LA CLASSIFICAZIONE AGID

Con la nota n. 2325 del 28 giugno scorso, il MIUR ha ricordato che, sulla base di quanto previsto negli artt. 3 e 5 del Regolamento AgID di cui alla Determinazione AgID n. 628/2021, tutte le Pubbliche Amministrazioni sono tenute a trasmettere l'elenco e la classificazione dei propri dati e servizi digitali all'Agenzia per la Cybersicurezza Nazionale, allo scopo di determinarne il livello di criticità. Al fine di adempiere al predetto obbligo, quindi, si invitano le scuole ad accedere alla piattaforma "Pa Digitale 2026" (raggiungibile a questo indirizzo web: PA digitale 2026), attivare il proprio profilo e completare la classificazione dei dati della scuola entro il termine prestabilito. Il processo di "**classificazione dei dati**" consiste nell'indicare quale tipologia di dati gestisce l'Istituzione Scolastica rispetto alla classificazione già prevista e che distingue i dati in 3 categorie:

- a. **dati strategici**: se la loro compromissione può determinare un pregiudizio alla sicurezza nazionali
- b. **dati critici**: se la loro compromissione può determinare un pregiudizio al mantenimento di funzioni rilevanti per la società, la salute, la sicurezza pubblica e il benessere economico e sociale del Paese
- c. **dati ordinari**: qualora la loro compromissione non determini i pregiudizi di cui alle lettere a) e b) Considerato che, salvo casi estremamente rari ed eccezionali, le scuole gestiscono "dati ordinari", al fine di semplificare il processo di "classificazione" è stato già predisposto sul portale "PA Digitale 2026" un elenco di n. 32 servizi di cui i dati sono stati automaticamente classificati come ordinari; salvo quindi eccezioni che prevedano l'aggiunta di nuovi servizi, al fine di adempiere all'obbligo predetto basterà confermare la classificazione pre-impostata entro il termine stabilito

LA CLASSIFICAZIONE GDPR

Posto quindi che i dati trattati dalle scuole tendenzialmente rientrano nella categoria dei dati "ordinari", ovvero dei dati che anche se violati non comportano impatti rilevanti sulla sicurezza nazionale, andiamo ora a vedere quali potrebbero essere gli impatti a livello personale. Già, perché la pubblicazione di un dato come, ad esempio, quello riguardante una malattia di uno studente o di un docente, può comportare grosse conseguenze in termini di riservatezza. Allo stesso modo la pubblicazione delle coordinate bancarie o dei criteri di economicità (ISEE in primis) che hanno portato alla qualificazione in una graduatoria. Tutte queste informazioni, se diffuse in modo errato, probabilmente non avranno ripercussioni sulla sicurezza nazionale, ma potrebbero portare anche ad effetti devastanti sulla vita degli individui, specie se minorenni. Proprio per tale motivo è necessario procedere con una classificazione e, possibilmente, con un'attività di labeling intesa come utilizzo di un determinato colore per distinguere le informazioni che possono essere diffuse da quelle che, invece, non possono esserlo.

A questo punto occorre evidenziare che la mappatura della tipologia dei dati trattati è già presente nel registro dei trattamenti risultando ridondante una ulteriore riproposizione della stessa anche in questa sede. Non solo, ai fini che ci stiamo qui proponendo, sono superflue



alcune distinzioni di dettaglio che potrebbero portare ad una estremizzazione della classificazione e, quindi, ad una difficile messa in atto della stessa. In tal senso, al fine di agevolare le operazioni di chi lavora nella scuola, riteniamo necessario suddividere tutte le informazioni nelle seguenti 3 categorie a cui associamo un label e una regola da rispettare:

CATEGORIA	LABEL (ETICHETTA)	REGOLA
NON DIVULGABILE	NESSUNA	<p>La regola generale è che le informazioni in possesso della scuola non possono essere divulgate a terzi, siano esse riconducibili a personale o a studenti. Per questo, trattandosi della normalità, possiamo evitare di etichettare le comunicazioni di questo tipo.</p> <p>Se una comunicazione non ha etichette di sorta alcuna deve ritenersi non divulgabile.</p>
AD USO INTERNO	GIALLA	<p>Esistono una moltitudine di informazioni utilizzabili solo per uso interno, solitamente tra il personale scolastico. Il riferimento è, ad esempio, al PEI, così come al nome e ai numeri di telefono dei genitori degli studenti, ma anche le graduatorie con indicazione di informazioni relative allo stato di salute (che dovrebbero essere omesse prima della pubblicazione in albo online).</p> <p>Si ricorda, a tal riguardo, che la pubblicazione online deve sempre essere preceduta da una richiesta di "doppio check" con il superiore, al fine di confermare il luogo e la modalità di pubblicazione prima che ciò avvenga.</p>
DIVULGAZIONE LIBERA	VERDE	<p>Si tratta delle informazioni che possono essere divulgate liberamente.</p> <p>Tra queste, sicuramente, un ruolo principale lo hanno quelle del tutto prive di dati personali (es: nomi e cognomi).</p>



COME ETICHETTARE

Esistono sistemi di etichettatura automatica delle e-mail. Ad ogni modo, nei casi di comunicazioni rientranti nella categoria gialla o verde è possibile anche solo inserire in oggetto la menzione dell'etichetta.

Esempio 1:

Destinatario: caio.sempronio@ilamiascuola.edu.it

Oggetto: [LABEL GIALLA] PEI Classe 4C

Caro Caio, ti allego.....

Esempio 2:

Destinatario: sempronio.tullio@lamiascuola.edu.it

Oggetto: [LABEL VERDE] Orario lezioni primo quadrimestre

Caro Sempronio, ti allego.....

