POLICY
PSEUDONIMIZZAZIONE E CIFRATURA DEI DATI

COD. C.08
VERS. 03 DEL 01.2026

CONTIENE:

INDICE DELLE VERSIONI SUCCESSIVE ALLA PRIMA:

COD. VERSIONE	DATA MODIFICA	MODIFICHE
02	25.07.2024	Integrazione sugli esempi di pseudonimizzazione e minori correzioni
03	03.01.2026	Unificazione con policy C.09 e aggiornamento normativo

PREMESSA

La presente Policy disciplina le misure tecniche e organizzative adottate dall'Istituzione scolastica al fine di garantire un adeguato livello di sicurezza dei dati personali e di ridurre il rischio di identificazione degli interessati, in conformità ai principi di liceità, correttezza, trasparenza, minimizzazione e integrità e riservatezza di cui agli articoli 5, 25 e 32 del Regolamento (UE) 2016/679 (di seguito, "GDPR").
Nel contesto scolastico, il trattamento di dati personali presenta profili di particolare delicatezza, anche in considerazione della frequente presenza di minori, della varietà delle finalità perseguite e dell'uso diffuso di strumenti digitali e piattaforme informatiche, talvolta fornite da soggetti stabiliti al di fuori dell'Unione europea. L'adozione di tecniche di anonimizzazione, pseudonimizzazione e cifratura costituisce pertanto una misura essenziale per prevenire violazioni dei dati personali e per limitare l'impatto di eventuali incidenti di sicurezza sui diritti e le libertà degli interessati. Mentre la pseudonimizzazione costituisce un metodo per occultare un dato personale, che consente in linea teorica di risalire all'informazione in chiaro tramite apposite procedure e informazioni aggiuntive, l'anonimizzazione è invece il risultato di un trattamento volto a impedire in modo irreversibile l'identificazione dell'interessato. Nel valutare se un trattamento consenta o meno l'identificazione di una persona fisica, i titolari e i responsabili del trattamento devono prendere in considerazione tutti i mezzi che possono essere "ragionevolmente utilizzati" per risalire all'identità, tenendo conto non solo delle proprie capacità, ma anche di quelle di terzi destinatari dei dati, come previsto dal GDPR e ribadito dalla giurisprudenza europea. In tale contesto si inserisce la recente e rilevante sentenza della Corte di Giustizia dell'Unione europea "Deloitte" (C-413/23 P), che ha chiarito come i dati pseudonimizzati non debbano essere automaticamente qualificati come dati personali in ogni circostanza e per ogni soggetto. La Corte ha infatti affermato che la qualificazione dei dati dipende da una valutazione concreta e caso per caso, fondata sull'effettiva possibilità di identificazione dell'interessato mediante mezzi ragionevolmente utilizzabili. In particolare, la Corte ha distinto la posizione del titolare del trattamento, che conserva le informazioni aggiuntive necessarie alla re-identificazione (e per il quale i dati restano personali), da quella del terzo destinatario che riceve i dati pseudonimizzati. Qualora quest'ultimo non disponga di alcun mezzo concreto, tecnico o giuridico, per risalire all'identità delle persone fisiche interessate, e le misure adottate rendano l'identificazione di fatto impossibile o sproporzionata, i dati possono non essere qualificati come personali nei suoi confronti. Ne consegue che non operano presunzioni assolute: la pseudonimizzazione può, a seconda delle circostanze, impedire effettivamente a soggetti diversi dal titolare di identificare l'interessato, con la conseguenza che, per tali soggetti, l'interessato non è o non è più identificabile.

Resta tuttavia fermo che, nella pratica, raggiungere una anonimizzazione pienamente definitiva è estremamente complesso. La letteratura di settore evidenzia come, disponendo di un numero sufficiente di dati e di adeguate capacità computazionali, anche informazioni apparentemente anonime possano essere ricondotte a una persona fisica. Pertanto, l'obiettivo realistico dell'anonimizzazione è quello di raggiungere un livello tale per cui la re-identificazione richiederebbe uno sforzo sproporzionato rispetto al contesto, alle finalità del trattamento e ai soggetti coinvolti. Nel contesto scolastico, la valutazione dello sforzo necessario per una eventuale de-anonimizzazione deve tenere conto dei destinatari concreti dei dati. Ad esempio, l'invio di informazioni anonimizzate a un genitore rende ragionevolmente improbabile l'utilizzo di strumenti sofisticati per l'identificazione; diversamente, la comunicazione di dati a soggetti dotati di elevate capacità tecnologiche potrebbe rendere necessario rivalutare l'efficacia delle tecniche adottate o, più radicalmente, la necessità stessa del trattamento. Considerata la complessità tecnica e organizzativa dei processi di anonimizzazione, nella gestione dei trattamenti scolastici risulta spesso più efficace fare riferimento alla corretta applicazione del principio di minimizzazione, limitando i dati trattati a quelli strettamente necessari rispetto alle finalità perseguite, e adottando misure di pseudonimizzazione adeguate, valutate alla luce del rischio concreto di identificazione.

AMBITO DI APPLICAZIONE

La presente Policy si applica a tutti i trattamenti di dati personali effettuati dall'Istituzione scolastica, indipendentemente dalla modalità di trattamento e dal supporto utilizzato, e vincola il Dirigente scolastico, il personale docente e il personale ATA, i collaboratori esterni, nonché eventuali fornitori che trattano dati personali per conto della scuola in qualità di responsabili del trattamento o di soggetti autorizzati.
Le disposizioni contenute nella presente Policy costituiscono parte integrante del Sistema di Gestione della Sicurezza delle Informazioni dell'Istituto e si affiancano alle ulteriori policy e procedure adottate in materia di protezione dei dati personali.

ANONIMIZZAZIONE

Per anonimizzazione si intende un trattamento dei dati personali volto a impedire in modo irreversibile l'identificazione dell'interessato. Un dato può considerarsi anonimizzato quando non consente, né direttamente né indirettamente, di risalire all'identità di una persona fisica mediante l'utilizzo di mezzi che possano essere ragionevolmente impiegati dal titolare del trattamento o da terzi, tenuto conto del contesto, delle finalità del trattamento e delle capacità tecniche disponibili.
Nel valutare l'effettiva idoneità di un processo di anonimizzazione, l'Istituzione scolastica tiene conto, tra l'altro, della tipologia dei destinatari dei dati, del volume e della natura delle informazioni trattate e del rischio concreto di re-identificazione. In considerazione delle difficoltà tecniche e organizzative connesse al raggiungimento di una anonimizzazione pienamente definitiva, l'anonimizzazione è adottata prioritariamente nei casi in cui la conoscenza dell'identità dell'interessato non sia necessaria per il perseguimento delle finalità del trattamento. In ambito scolastico, l'anonimizzazione trova applicazione, in particolare, nei casi di comunicazione o pubblicazione di documenti verso soggetti esterni all'organizzazione, nelle procedure di accesso agli atti e di accesso civico, nelle attività di pubblicità legale e trasparenza decorso il termine di legge, nonché nelle comunicazioni di carattere generale rivolte a una pluralità indeterminata di destinatari, quali le comunicazioni scuola–famiglia relative a situazioni non individualizzate. L'anonimizzazione deve essere realizzata mediante tecniche idonee a garantire la rimozione effettiva e non reversibile delle informazioni identificative, evitando soluzioni meramente apparenti che consentano il recupero dei dati originari.

PSEUDONIMIZZAZIONE

La pseudonimizzazione consiste nel trattamento dei dati personali in modo tale che essi non possano essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive. Tali informazioni aggiuntive devono essere conservate separatamente e protette mediante adeguate misure tecniche e organizzative, al fine di impedire l'identificazione non autorizzata degli interessati.

Nel contesto scolastico, la pseudonimizzazione è adottata quando l'identificazione diretta dell'interessato non risulta necessaria per il perseguimento delle finalità del trattamento, ma permane l'esigenza di mantenere un collegamento, seppur indiretto, con la persona cui il dato si riferisce. Ciò avviene, ad esempio, nelle comunicazioni tra docenti, nella condivisione di documenti didattici, nella gestione di attività educative o organizzative e nell'utilizzo di piattaforme digitali e ambienti di lavoro collaborativi. La chiave di collegamento tra il dato pseudonimizzato e l'identità reale dell'interessato deve essere accessibile esclusivamente a soggetti espressamente autorizzati, quali il Dirigente scolastico o il personale di segreteria, e deve essere conservata in un ambiente distinto rispetto ai dati pseudonimizzati. È fatto divieto di adottare forme di pseudonimizzazione solo apparenti, quali l'utilizzo di sigle facilmente riconducibili all'interessato o di codici basati su elementi evidenti, nonché di conservare le informazioni aggiuntive nello stesso documento o nella medesima cartella dei dati pseudonimizzati. La pseudonimizzazione costituisce una misura di protezione idonea a ridurre i rischi per i diritti e le libertà degli interessati, ma non comporta la perdita della natura di dato personale ai sensi del GDPR per il titolare del trattamento che conserva le informazioni necessarie alla re-identificazione.

BENEFICI DELLA PSEUDONIMIZZAZIONE

La pseudonimizzazione permette di:

- Nascondere l'identità dei soggetti, a cui i dati sono riferiti, a chiunque non ne sia autorizzato (terze parti), pur mantenendo la congruità semantica di ciascun dataset (dataset pseudonimizzato/dataset di transcodifica).
- Garantire il rispetto dei principi della minimizzazione del dato e del "*need to know*", laddove le informazioni relative all'identificazione del soggetto interessato non siano necessarie, ad esempio, alle finalità del trattamento. La separazione del dataset pseudonimizzato dalla tabella di transcodifica consente di soddisfare i requisiti normativi imposti dagli artt. 4, 5, 25 e 32 del GDPR, limitando l'accesso alle sole informazioni necessarie al trattamento.

ESEMPI DI PSEUDONIMIZZAZIONE

Sebbene la pseudonimizzazione così come descritta dal GDPR e dalle *best practice* ENISA sia una misura tecnica ed organizzativa di non facile implementazione da parte delle scuole, è opportuno comunque focalizzare una serie non

esaustiva di casi nei quali dovrebbe essere utilizzata al fine di ridurre il più possibile i rischi di *data breach* e, al contempo, contenere i rischi dei trasferimenti di dati extra UE connessi all'utilizzo di Google Workspace:

1. **Pseudonimizzazione degli indirizzi e-mail degli alunni**: questa misura di protezione prevede che la scuola abbia implementato un regolamento informatico che indichi espressamente, tra le altre cose, il soggetto responsabile a mettere in atto questa misura, quale logica è stata utilizzata per creare gli pseudonimi, per quale tipologia di utenti viene utilizzata, chi si trova in possesso delle informazioni aggiuntive per accedere ai dati personali, le tempistiche di revisione della procedura.
2. **Pseudonimizzazione dei PDP/PEI in Google Workspace**: strutturare i PDP e i PEI con i dati in chiaro in Google Workspace è molto rischioso per i diritti e le libertà degli interessati. Sebbene la piattaforma costituisca uno strumento di lavoro molto potente, va utilizzata mettendo in atto tutte le misure tecniche ed organizzative del caso per poter operare nella legalità. Non è *privacy compliant* associare i PDP/PEI all'interessato Mario Rossi o M.R. poiché l'alunno potrà essere facilmente identificabile da Google; risulta invece *privacy compliant* adottare delle vere e proprie procedure di pseudonimizzazione, descrittive della fase di strutturazione, comunicazione, conservazione e archiviazione dei dati, come l'implementazione di soluzioni di crittografia lato *client*, che consentono di crittografare le informazioni sui dispositivi *client* prima di essere inviate ai server di Google. Per la validazione di queste procedure è opportuno contattare, oltre ai tecnici informatici, anche il DPO.
3. **Pseudonimizzazione delle comunicazioni e-mail**: è opportuno che il personale scolastico si abitui, ove possibile, a rendere le comunicazioni tramite e-mail il meno identificabili possibili utilizzando quantomeno delle forme di pseudonimizzazione (ad esempio: anziché Mario Rossi riportare M.R.) o, meglio ancora dei veri e propri pseudonimi.

PROCESSO	TECNICA DI PSEUDONIMIZZAZIONE	MISURE DA ATTUARSI
INDIRIZZI E-MAIL	COMPLESSA	COSTITUZIONE DI UN REGOLAMENTO INFORMATICO
PEI/PDP	COMPLESSA	IMPLEMENTAZIONE DI ADEGUATE PROCEDURE TECNICHE E ORGANIZZATIVE VALIDATE DAL DPO
COMUNICAZIONI E-MAIL	SEMPLICE	INDICAZIONI DEL DIRIGENTE SCOLASTICO E DEL DPO
INDICARE PROCESSO		

DIFFERENZA TRA PSEUDONIMIZZAZIONE BY DESIGN E CIFRATURA

La cifratura (*encryption*) è un processo di offuscamento del dato che, mediante l'impiego di un algoritmo matematico, restituisce un output non intellegibile da parte di un utente che non possiede la chiave di decifratura. La cifratura è quindi un particolare processo di pseudonimizzazione, che presenta le seguenti caratteristiche: *(i)* a partire da un dataset iniziale ne restituisce esclusivamente uno cifrato; (*ii*) le informazioni cifrate sono completamente non intellegibili da un soggetto terzo, viene meno la riconducibilità al dato originale e il valore semantico del dato stesso.

Come per la pseudonimizzazione, la crittografia è una misura di protezione di non facile predisposizione. Ciò nonostante, la crittografia può trovare applicazione in forma semplice in alcuni trattamenti di dati messi in atto dal personale scolastico.

PROCESSO	TECNICA DI CRITTOGRAFIA	MISURE DA ATTUARSI
Memorizzazione dei dati su chiavetta USB	Crittografia simmetrica	Utilizzo di chiavette crittografate o inserimento di password sulla singola cartella o sul singolo file
Comunicazione di elenchi di dati personali via e-mail	Crittografia simmetrica	Inserimento di password sul singolo file con comunicazione della stessa attraverso mezzo diverso
INDICARE PROCESSO		

Si fa inoltre presente che, in caso di perdita o furto di dispositivo i cui dati non siano stati crittografati, sarà comunque necessario non solo documentare la perdita del dispositivo all'interno del registro delle violazioni, ma anche comunicare il *data breach* al Garante per la Protezione dei Dati Personali.

	REGISTRO DELLE VIOLAZIONI	COMUNICAZIONE AL GARANTE	COMUNICAZIONE AGLI INTERESSATI
DISPOSITIVO CON DATI NON CRITTOGRAFATI	SÌ	SÌ	Non esclusa qualora sulla chiavetta siano eventualmente (anche se non dovrebbero) conservati categorie particolari di dati personali
DISPOSITIVO CON DATI CRITTOGRAFATI	SÌ	NO	NO

PRINCIPIO DI MINIMIZZAZIONE

L'adozione delle tecniche di anonimizzazione, pseudonimizzazione e cifratura deve avvenire nel rispetto del principio di minimizzazione dei dati, limitando il trattamento alle sole informazioni strettamente necessarie rispetto alle finalità perseguite. In molti casi, la corretta applicazione della minimizzazione, unitamente alla pseudonimizzazione e alla cifratura, consente di ridurre significativamente i rischi connessi al trattamento, evitando la necessità di trattare dati identificativi completi. Le misure di cui alla presente Policy possono essere adottate anche in modo combinato, in funzione del contesto del trattamento, dei destinatari dei dati e del livello di rischio individuato, sulla base di una valutazione preventiva effettuata dal Titolare del trattamento con il supporto del Responsabile della Protezione dei Dati.

COME ANONIMIZZARE

Sono numerose e anche molto complesse le tecniche di anonimizzazione conosciute nella letteratura di settore. Per quanto riguarda il mondo della scuola è da ritenere sufficiente la cancellazione fisica (ad esempio: con pennarello o con funzione cancella del compilatore Word) dei nominativi e dei dati di contesto che consento di identificare un soggetto.

Esempio: "il soggetto Tizio Caio ha votato sì" può diventare "il soggetto [omissis] ha votato sì".

Un'altra metodologia piuttosto semplice per raggiungere un buon grado di anonimizzazione prevede di utilizzare dati anonimi e aggregati. In questo caso, il dato viene prima privato di riferimenti nominativi e poi viene, per l'appunto, aggregato a quello di altri soggetti previamente anonimizzati.

Esempio: "il soggetto Tizio ha votato sì; il soggetto Caio ha votato no; il soggetto Sempronio ha votato sì; il soggetto Mevio ha votato no" diventa "due soggetti hanno votato sì e due soggetti hanno votato no".

Si tratta di un'operazione piuttosto semplice che porta ad un risultato già di per sé accettabile se parliamo del mondo scolastico.

COME PSEUDONIMIZZARE

Nel contesto scolastico, la pseudonimizzazione può essere realizzata mediante la sostituzione del nome e del cognome dell'alunno con un codice identificativo, una sigla o un riferimento interno, purché la chiave di collegamento tra codice e identità reale sia conservata separatamente e protetta.

Esempio: "l'alunno Tizio Caio ha ottenuto la valutazione X" può diventare "l'alunno ID_23A ha ottenuto la valutazione X".

La tabella di corrispondenza tra l'identificativo (ID_23A) e il nominativo dell'alunno deve essere:

- conservata in un ambiente distinto rispetto al documento pseudonimizzato;
- accessibile solo a soggetti espressamente autorizzati (ad es. Dirigente scolastico, segreteria);
- protetta mediante adeguate misure di sicurezza tecniche e organizzative.

La pseudonimizzazione può essere utilizzata, ad esempio, nelle comunicazioni tra docenti, nella condivisione di documenti su drive o in contesti in cui non sia necessario conoscere l'identità completa dell'interessato per il perseguimento della finalità.

È necessario evitare forme di pseudonimizzazione solo apparenti, quali:

- l'utilizzo di sigle facilmente riconducibili all'interessato;
- l'impiego di codici basati su elementi evidenti (iniziali del nome e cognome, data di nascita, classe);
- la conservazione della chiave di collegamento nello stesso documento o nella stessa cartella del file pseudonimizzato.

La pseudonimizzazione deve essere applicata nel rispetto del principio di minimizzazione e tenendo conto dei soggetti che possono accedere ai dati, affinché l'identificazione dell'interessato non sia possibile se non per chi sia legittimato a farlo.

UTILIZZO DI PROGRAMMI INFORMATICI DI ANONIMIZZAZIONE A NORMA

Per procedere all'anonimizzazione dei dati personali contenuti in taluni documenti – quali, a titolo esemplificativo, i curriculum vitae di esperti esterni o le dichiarazioni di assenza di conflitto di interessi o di incompatibilità – devono essere utilizzati programmi informatici adeguati, idonei a garantire la rimozione effettiva e non reversibile delle informazioni identificative. Non è consentito scaricare i documenti, procedere a una anonimizzazione manuale e successivamente ricaricarli online, in quanto tali modalità non assicurano la reale eliminazione dei dati personali. Nell'ambito dei processi di digitalizzazione documentale, l'anonimizzazione deve avvenire mediante procedure digitali strutturate, in grado di impedire il recupero del contenuto originario. In particolare, non è consentito fare affidamento sull'annerimento del testo tramite funzioni di evidenziazione grafica (ad esempio evidenziazione in colore nero), poiché tale modalità non comporta la cancellazione del testo sottostante, che può essere facilmente recuperato attraverso operazioni di copia, selezione o rielaborazione del file. Analogamente, l'oscuramento del testo mediante pennarello o strumenti manuali non è considerato sufficiente, qualora non garantisca la completa e irreversibile eliminazione delle informazioni personali. Il personale è tenuto a utilizzare esclusivamente software autorizzati, secondo le indicazioni fornite dall'amministratore di sistema. A titolo esemplificativo, possono essere impiegati strumenti quali PDF24, doPDF o Adobe Acrobat Pro, configurati in conformità alle politiche di sicurezza dell'istituto. È fatto espresso divieto di utilizzare servizi o applicazioni che comportino la trasmissione dei documenti a piattaforme esterne non autorizzate, quali servizi di elaborazione online dei file (ad esempio "I Love PDF"), in quanto non adeguati al contesto della Pubblica Amministrazione.

CASISTICHE DI ANONIMIZZAZIONE A SCUOLA

ACCESSO AGLI ATTI DI PROCEDIMENTO DISCIPLINARE

Il caso principale in cui si chiede ad un istituto scolastico di procedere anonimizzando un dato è quello relativo all'invio di documenti a terzi. Qui, ove possibile, è opportuno anonimizzare le informazioni da inviare o quanto meno renderle non riconducibili ad una persona fisica, come descritto nella citata Sentenza "Deloitte". Un esempio ci arriva dalla giurisprudenza del TAR (sentenza numero 09974/2018) ove si legge che, in caso di procedimento disciplinare a carico di un alunno, egli ha la possibilità di domandare l'accesso ai dati (testimonianze di colleghi) che hanno orientato il procedimento disciplinare stesso e che, tuttavia, la scuola ha il diritto di inviare questi documenti previa anonimizzazione degli stessi. Attenzione, alla scuola in questo caso non si chiede solo di cancellare i nomi ma si chiede di cancellare ogni riferimento che possa ricondurre al soggetto interessato. Per capirci, se parla l'unico alunno presente in classe in un determinato momento, non sarà sufficiente eliminare il nominativo ma sarà necessario eliminare ogni riferimento che possa ricondurre alla sua identità.

ACCESSO AGLI ATTI DI GRADUATORIE

Prima di procedere, precisiamo che la gestione di un accesso ai dati è sempre da valutare caso per caso, bilanciando diritti e doveri di tutte le parti in causa. Ciò detto, è possibile che un soggetto richieda di accedere agli atti (ad esempio: documenti medici di parenti di docenti) che hanno orientato le graduatorie. In questo caso, salvo che esista un interesse concreto ed attuale alla conoscenza del nome dei parenti, il richiedente sarà soddisfatto anche con la consegna di un documento anonimo.

SCADENZA DEI TERMINI DI LEGGE PER LE PUBBLICAZIONI AI FINI DELLA PUBBLICITÀ LEGALE E DELLA TRASPARENZA

Gli addetti alla pubblicazione devono assicurarsi di oscurare se del caso anonimizzando i dati e le informazioni che non devono essere più visibili agli esterni all'organizzazione al decorrere dei termini previsti dalla legge per gli atti e i documenti pubblicati ai fini della pubblicità legale e della trasparenza. L'anonimizzazione dei dati potrebbe inoltre essere applicata a seguito di richiesta di cancellazione dei dati proveniente da parte degli interessati. Si rimanda alla policy sulla pubblicazione dei documenti.

COOKIE ANONIMI

Non è mai semplice la gestione dei cookie su un sito scolastico. Quello che ci interessa qui sapere (rinviando all'apposita policy sito per ogni ulteriore info) è che la presenza di cookie analitici comporta adempimenti sproporzionati rispetto alle effettive finalità che potrebbe avere un istituto scolastico. Per questo, è caldamente suggerito alle scuole di anonimizzare i cookie analitici utilizzando le apposite funzioni all'uopo realizzate dai principali fornitori di simili tecnologie. Questo permette, tra l'altro, di avere informazioni interessanti quali il numero, la provenienza e il percorso degli utenti del nostro sito, senza tuttavia conoscerne i nomi, evitando quindi inutili trattamenti che spesso comportano adempimenti quali, a titolo esemplificativo: la creazione di apposito banner cookie; la predisposizione di un cookie manager; la creazione di una informativa ad hoc ecc. A prescindere dall'istanza dell'interessato, in base alle indicazioni del Garante Privacy è previsto che, entro un termine prestabilito caso per caso, la scuola è tenuta a rendere non accessibili/visibili dati/documenti a soggetti esterni.

ANONIMIZZAZIONE DEI DATI NELLE RICHIESTE DI ACCESSO CIVICO

Nel caso delle istanze di accesso civico generalizzato delle ditte che hanno partecipato ai bandi/manifestazioni di interesse relativi alle forniture delle bevande, le istanze potranno essere accolte previa anonimizzazione di tutti i documenti di identità dei rappresentanti legali che hanno partecipato ai bandi/manifestazioni.

ANONIMIZZAZIONE DEI DATI SENSIBILI NELLE PIATTAFORME AMERICANE

Per garantire un adeguato livello di protezione dei dati personali, la strutturazione e la conservazione dei PEI/PDP all'interno dei servizi di archiviazione cloud forniti da piattaforme extra-UE (c.d. "piattaforme americane") devono avvenire applicando prioritariamente il principio di minimizzazione dei dati di cui all'art. 5, par. 1, lett. c) GDPR. Considerata la complessità tecnica e organizzativa dell'anonimizzazione definitiva, nonché l'esigenza di non ostacolare l'operatività dei docenti, la scuola adotta una modalità di trattamento basata sulla riduzione preventiva delle informazioni personali contenute nei documenti archiviati sul Drive. In particolare, i PEI/PDP depositati sulle piattaforme cloud devono contenere esclusivamente i dati strettamente necessari allo svolgimento dell'attività didattica, quali il nome, il cognome e la classe di appartenenza dell'alunno, evitando l'inserimento di ulteriori dati personali o identificativi, quali, a titolo esemplificativo e non esaustivo, data e luogo di nascita, codice fiscale, residenza, cittadinanza, data di ingresso in Italia o altre informazioni anagrafiche e sensibili. I dati ulteriori, necessari per finalità amministrative o di segreteria, non devono essere archiviati in forma completa sulle piattaforme cloud, ma gestiti tramite i sistemi informativi interni della scuola o altri canali autorizzati, nel rispetto delle misure di sicurezza previste. Attenzione: nella fase di trasmissione dei PEI/PDP alla segreteria, il documento deve essere scaricato dal Drive su una postazione informatica della scuola, integrato localmente con i dati personali necessari e successivamente trasmesso alla segreteria tramite i canali istituzionali previsti. Una volta completata la trasmissione, il file contenente i dati personali completi deve essere tempestivamente cancellato dalla postazione utilizzata, al fine di evitare duplicazioni non necessarie e ridurre il rischio di accessi non autorizzati.

ANONIMIZZAZIONE DELLE COMUNICAZIONI SCUOLA - FAMIGLIA

Le FAQ dell'Autorità Garante per la protezione dei dati personali, con riferimento alle comunicazioni scuola–famiglia, stabiliscono espressamente che nelle circolari, nelle delibere e, più in generale, in tutte le comunicazioni non rivolte a destinatari specificamente individuati, non devono essere inseriti dati personali idonei a rendere identificabili gli alunni, in particolare quando le informazioni riguardino situazioni delicate, quali episodi di bullismo, l'irrogazione di sanzioni disciplinari o altre vicende di natura sensibile. Tale indicazione assume carattere vincolante ai fini della corretta applicazione della normativa in materia di protezione dei dati personali. Pertanto, l'inserimento in comunicazioni di carattere generale di informazioni che consentano, anche indirettamente, l'identificazione degli interessati espone l'istituzione scolastica al rischio di reclami, accertamenti ispettivi e sanzioni, nonché il personale coinvolto a possibili responsabilità disciplinari, in relazione al mancato rispetto delle istruzioni impartite dal Titolare del trattamento e delle disposizioni dell'Autorità di controllo. Resta fermo che, nelle comunicazioni interne di natura amministrativa o gestionale, indirizzate a destinatari specificamente individuati e legittimati (quali la segreteria scolastica o il Dirigente scolastico), è consentito e necessario inserire i dati personali strettamente utili all'identificazione dell'interessato, nel rispetto del principio di minimizzazione e delle misure di sicurezza previste. Ne consegue che l'anonimizzazione o la minimizzazione dei dati deve essere applicata in modo sistematico nelle comunicazioni tra docenti, nonché nelle comunicazioni rivolte alle famiglie o a una pluralità indeterminata di destinatari, mentre l'utilizzo di dati identificativi completi è ammesso esclusivamente nei flussi informativi interni, limitati a soggetti autorizzati e per finalità istituzionali chiaramente determinate.