

**Vargiu Scuola Srl**

Via dei Tulipani 7/9 – Assemini (CA) - 09032

Sito: vargiuscuola.it

commerciale@vargiuscuola.it

tel: 070271526, 070271560

partita iva: 03679880926

*Alle scuole iscritte alla mailing list di
informazione gratuita curata da Vargiu Scuola*

VS_SVR 104/2026

Assemini, 20/9/2026

Registro Elettronico all'avvio dell'anno scolastico 2026/27: accessi, aree riservate e dati particolari degli alunni

Con l'avvio dell'anno scolastico 2026/27 il Registro Elettronico torna al centro dell'organizzazione di ogni istituzione scolastica: si aprono le abilitazioni per i nuovi utenti, si ricompongono i consigli di classe e riprende la condivisione quotidiana di informazioni fra i docenti e con i genitori e gli alunni. Negli ultimi mesi abbiamo dedicato al Registro diverse note: la [DPO 6/2026](#) sulle novità introdotte dall'art. 51 della Legge 182/2025, la [DPO 17/2026](#) sull'uso di SPID e CIE da parte degli studenti minorenni e, da ultimo, la [DPO 97/2026](#), con le indicazioni operative e i modelli per il passaggio definitivo all'identità digitale. Nella nota [DPO 103/26](#) abbiamo invece fornito la nostra guida operativa per rispondere alla richiesta di accesso civico generalizzato presentato da una giornalista a tanti istituti scolastici relativamente all'uso del Registro elettronico.

La presente nota perché riteniamo che siano ancora troppe le violazioni di dati personali che si verificano nel Registro Elettronico e che il Garante non manca di sanzionare. Nella nostra esperienza di DPO esse hanno origine, per lo più, da due cause: i **furti di identità**, resi possibili da credenziali tradizionali sottratte ai relativi proprietari e gli **errori commessi nel caricamento dei documenti**, primi fra tutti PEI e PDP resi visibili, per una scelta sbagliata dell'area o dei destinatari, a genitori che non avrebbero dovuto conoscerli. Si tratta di incidenti evitabili. L'accesso al Registro mediante le identità digitali SPID e CIE rende di fatto impraticabile l'uso delle credenziali altrui, mentre le tecniche di pseudonimizzazione e di cifratura dei documenti, di cui parleremo più avanti, fanno sì che un errore nel caricamento non si traduca nella conoscibilità dei dati da parte di chi non è autorizzato. Sono queste le misure che consentono alla scuola di continuare a utilizzare il Registro come primo strumento di condivisione di informazioni e documenti fra docenti, genitori e alunni, senza doverne limitare l'uso per timore dell'errore.

1. Personale scolastico e genitori: l'identità digitale come regola

L'accesso al Registro Elettronico mediante SPID o CIE è previsto dalla legge. L'art. 51 della Legge 2 dicembre 2025, n. 182, modificando l'art. 7, comma 31, del D.L. 95/2012, dispone che «*ai registri online si accede tramite il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID) o la carta di identità elettronica (CIE)*», dando veste legislativa a un indirizzo che il Ministero dell'Istruzione e del Merito aveva più volte espresso con la circolare 4588 dell'8/11/2023, con la [nota 4717 del 12/9/2024](#) e con la [nota 2773 del 4/4/2025](#).

Per il personale scolastico la regola va applicata senza eccezioni. Il Dirigente Scolastico dispone, con proprio atto organizzativo, che docenti e personale ATA accedano al Registro **esclusivamente con la propria identità digitale**, e chiede al fornitore la disattivazione delle credenziali tradizionali: abilitare SPID e CIE lasciando attivo, in parallelo, il canale nome utente/password non produce alcun beneficio in termini di sicurezza. L'identità digitale è ormai una dotazione professionale ordinaria del dipendente pubblico, che la utilizza per NoiPA, Istanze OnLine e gli altri servizi dell'amministrazione, e tutela in primo luogo il dipendente, rendendo certa la riconducibilità delle operazioni compiute sul Registro al loro effettivo autore.

Anche per i genitori l'accesso con SPID o CIE deve costituire la **modalità ordinaria**, da comunicare alle famiglie e da applicare a tutte le nuove abilitazioni. Poiché tuttavia la scuola non dispone nei confronti delle famiglie di alcun potere organizzativo, e poiché il Registro è il canale ordinario di comunicazione fra scuola e famiglia, occorre evitare che la mancanza dell'identità digitale si traduca nell'impossibilità di esercitare consapevolmente la responsabilità genitoriale. La scuola deve quindi adottare una procedura documentata che consenta al genitore oggettivamente impossibilitato all'uso di SPID o CIE di richiedere il rilascio di credenziali: richiesta scritta e motivata, valutazione del Dirigente Scolastico, abilitazione di durata limitata all'anno scolastico, registrazione delle abilitazioni rilasciate e avvertenza sul divieto di cedere le credenziali a terzi, compreso il figlio minore. Gli elementi della procedura e i relativi modelli (circolari al personale, comunicazione alle famiglie, modulo di richiesta delle credenziali) sono contenuti nella nota [DPO 97/2026](#), alla quale rinviamo.

2. Gli alunni del primo ciclo: che cosa la legge riserva ai genitori

L'art. 51, comma 8, della Legge 182/2025 stabilisce che «*nel primo ciclo di istruzione alle comunicazioni in formato elettronico accedono i genitori degli alunni o gli esercenti la responsabilità genitoriale*». La disposizione è stata talvolta letta come un divieto generalizzato di accesso degli alunni al Registro. Si tratta, a nostro avviso, di un'interpretazione che va oltre il testo della norma.

Oggetto della disposizione sono le **comunicazioni fra scuola e famiglia**: circolari e avvisi alle famiglie, valutazioni, assenze e giustificazioni, annotazioni disciplinari, comunicazioni individuali, prenotazione dei colloqui. Queste informazioni sono destinate ai genitori, che devono riceverle direttamente dalla scuola e non per il tramite del figlio, e l'alunno del primo ciclo non potrà accedervi con le proprie credenziali. Ciò non significa, però, che l'alunno non possa utilizzare il Registro per lo svolgimento delle attività didattiche e per lo scambio di informazioni con i docenti, i quali possono servirsi per fornire materiale didattico, indicare gli argomenti delle lezioni e assegnare i compiti per casa. Questi ultimi andranno sempre riportati anche sul diario cartaceo, come raccomandato dalle note ministeriali [5274 dell'11/7/2024](#) e [2773 del 4/4/2025](#): il Registro affianca il diario, ma non può sostituirlo come strumento con il quale l'alunno prende nota dei propri impegni.

In questa prospettiva va letta anche l'indicazione contenuta al paragrafo 7 della nota [DPO 97/2026](#): ciò che nel primo ciclo va escluso non è necessariamente il profilo «studente» in quanto tale, ma l'accesso dell'alunno alle sezioni dedicate alle comunicazioni scuola-famiglia intese come scuola - genitori. La scuola che intenda mantenere per gli alunni un profilo limitato alle funzioni didattiche lo stabilirà con atto espresso del Dirigente Scolastico o nel regolamento d'istituto, indicando le sezioni visibili, e ne darà informazione alle famiglie; la guida per gli studenti allegata alla nota 97/2026 ([allegato 4](#)) è predisposta proprio per questa ipotesi. In ogni caso l'alunno accede con credenziali proprie e mai con quelle del genitore.

3. SPID e CIE per gli alunni: una scelta rimessa alla scuola

Le disposizioni vigenti consentono l'uso dell'identità digitale anche ai minori: lo SPID può essere attivato a partire dai 5 anni di età, con il consenso dei genitori, secondo le linee guida AgID per il rilascio dell'identità digitale ai minori, mentre la CIE può essere rilasciata fin dalla nascita. Il Gateway delle identità messo a disposizione dal Ministero supporta espressamente lo SPID per minori e l'uso della CIE da parte degli studenti minorenni, come abbiamo illustrato nella nota [DPO 17/2026](#).

Che lo strumento sia disponibile non significa tuttavia che debba essere imposto. Sarà la scuola a valutare se l'accesso degli alunni al Registro debba avvenire mediante SPID, CIE o credenziali rilasciate dalla scuola stessa, e il criterio di maggiore rilievo nella scelta è ovviamente l'età. Nelle scuole del primo ciclo l'uso di SPID e CIE può apparire eccessivamente prematuro, anche considerando che richiede di norma la disponibilità di un dispositivo personale, in genere lo smartphone sul quale è installata l'app del gestore dell'identità digitale o l'app CielD, di cui molti alunni non dispongono o del quale le famiglie ritengono non ancora opportuno un uso autonomo. In questi casi l'accesso dell'alunno alle sole aree

didattiche mediante credenziali rilasciate dalla scuola rappresenta una soluzione ragionevole e proporzionata, ferma restando per i genitori la regola dell'identità digitale.

Diverso è il discorso per le scuole secondarie di secondo grado, dove l'accesso mediante SPID e CIE assume anche una **valenza formativa**: gli studenti, prossimi alla maggiore età, devono imparare a utilizzare correttamente la propria identità digitale per rapportarsi con una pubblica amministrazione sempre più digitalizzata, dall'iscrizione all'università ai servizi sanitari, previdenziali e fiscali. L'uso quotidiano del Registro è un'occasione concreta per acquisire questa competenza, in coerenza con gli obiettivi dell'educazione alla cittadinanza digitale; resta ferma la possibilità di mantenere in via transitoria le credenziali per gli studenti che incontrino difficoltà nell'attivazione dell'identità digitale.

4. Le aree riservate del Registro: a ciascuna il suo contenuto

Il Registro Elettronico non è uno spazio unico di comunicazione. La sua corretta configurazione presuppone che siano presenti, e chiaramente riconoscibili, ambienti riservati allo scambio di informazioni fra soggetti diversi: l'area condivisa fra i **docenti componenti del consiglio di classe**; l'area di comunicazione fra **docenti e genitori**, dalla quale gli alunni restano esclusi, soprattutto nelle scuole del primo ciclo; l'area di comunicazione fra **docenti e studenti**. All'interno di ciascun ambiente la visibilità dei contenuti può essere ulteriormente modulata: un documento destinato alle famiglie può essere reso visibile ai genitori di un singolo alunno oppure a tutti i genitori della classe, e la differenza fra le due opzioni è spesso affidata a un solo segno di spunta (con le conseguenti possibilità di errore).

Ogni docente deve avere piena consapevolezza di questi ambienti di comunicazione separati e piena chiarezza di che cosa possa essere condiviso in ciascuno di essi. Sono ancora troppi i data breach che ci vengono segnalati, nel nostro ruolo di DPO, per il caricamento di informazioni riservate degli alunni nella parte del Registro accessibile a tutti i genitori. Un esempio ricorrente riguarda la materia disciplinare: **i richiami, le segnalazioni sul comportamento e gli atti relativi ai procedimenti disciplinari vanno collocati esclusivamente nell'area condivisa con i colleghi del consiglio di classe**, mentre il provvedimento eventualmente adottato va portato a conoscenza dei soli genitori dell'alunno interessato, con comunicazione individuale, e mai nella bacheca o nelle sezioni visibili a tutte le famiglie della classe.

La tabella che segue riassume, per le principali tipologie di informazioni, a chi devono essere rese accessibili.

Informazione / documento	Docenti del consiglio di classe	Genitori dell'alunno interessato	Tutte le famiglie della classe
Argomenti delle lezioni, compiti assegnati, materiali didattici	Sì	Sì	Sì (visibili anche agli alunni nell'area didattica)
Avvisi e comunicazioni organizzative alla classe (orari, uscite, iniziative)	Sì	Sì	Sì
Voti, valutazioni e documento di valutazione	Sì	Sì	No
Assenze, ritardi e giustificazioni	Sì	Sì	No
Prenotazione ed esito dei colloqui	Sì	Sì	No
Annotazione o provvedimento disciplinare adottato	Sì	Sì (comunicazione individuale)	No
Richiami, segnalazioni sul comportamento, atti istruttori dei procedimenti disciplinari	Sì	No	No
Osservazioni sui singoli alunni, documenti di lavoro e verbali delle sedute riservate ai docenti	Sì	No	No
Informazioni sulla situazione familiare o sociale dell'alunno	Sì (solo se necessarie)	No	No
PEI, PDP, diagnosi, certificazioni e altri documenti con dati sulla salute	Sì (solo documenti protetti, v. par. 5)	Sì (consegna diretta o comunicazione individuale protetta)	Mai

La tabella va letta insieme a una regola di comportamento elementare, che suggeriamo di richiamare espressamente nella circolare ai docenti: prima di pubblicare qualunque contenuto riferito a un singolo alunno occorre verificare l'area nella quale lo si sta inserendo e i destinatari selezionati, senza fare affidamento sulle impostazioni predefinite dell'applicativo; nel dubbio, il contenuto non si pubblica e ci si rivolge al coordinatore di classe o alla segreteria.

Se per errore un contenuto viene reso visibile a destinatari non autorizzati, il docente deve rimuoverlo immediatamente e informare senza ritardo il Dirigente Scolastico, che valuterà con il DPO la necessità della notifica al Garante entro 72 ore dalla conoscenza dell'evento (art. 33 del GDPR). Nel caso deciso dal Garante con il provvedimento del 27 febbraio 2025, di cui diremo nel paragrafo successivo, l'errore era stato corretto dopo 22 minuti, ma nessuno aveva ritenuto di avvisare il dirigente, che ne era venuto a conoscenza oltre due mesi dopo a seguito di una lettera del legale della famiglia.

Definire procedura

Mettere link nota che tratta gestione databreach

5. I dati particolari nel Registro: pseudonimizzazione e cifratura

La cautela nella condivisione di informazioni sul Registro deve essere massima quando si trattano dati particolari, in primo luogo i dati relativi alla salute e alla disabilità degli alunni (art. 9 del GDPR). Non è purtroppo raro l'incidente causato dal docente che carica sul Registro documenti come il PEI o il PDP in aree non riservate ai docenti, ma accessibili ai genitori della classe. Si tratta di violazioni gravi della normativa, che il Garante non manca di censurare.

Un caso emblematico è quello deciso con il [Provvedimento del 27 febbraio 2025 \[doc. web n. 10126123\]](#): una docente di sostegno della scuola primaria, nell'inserire il PEI di un alunno nella sezione di condivisione documenti per renderlo disponibile ai genitori, aveva selezionato per errore anche la classe, rendendo il documento visibile a tutti i genitori per circa 22 minuti. Il Garante ha dichiarato l'illiceità del trattamento per violazione degli artt. 5, par. 1, lett. a), 6 e 9 del GDPR e degli artt. 2-ter e 2-sexies del Codice, qualificando l'accaduto come comunicazione di dati relativi alla salute a soggetti terzi, e ha ammonito l'istituto, precisando che non rilevava la circostanza, addotta dalla scuola, che la condizione dell'alunno fosse già nota ai compagni di classe.

Il provvedimento merita però una lettura attenta. Il Garante non contesta alla scuola di avere utilizzato il Registro per condividere il PEI, né afferma che documenti contenenti dati particolari non possano transitare dal Registro: la violazione è individuata nell'errore commesso nel momento in cui l'informazione è stata portata a conoscenza di soggetti non autorizzati. È significativo che la scuola, dopo l'accaduto, abbia vietato qualsiasi condivisione digitale di PEI e PDP: una scelta comprensibile nell'immediatezza dell'evento, ma non imposta dalla decisione dell'Autorità, che priva il consiglio di classe di uno strumento utile e rischia di spostare la circolazione dei documenti su canali meno controllati, quali la posta elettronica personale, le chiavette USB o le applicazioni di messaggistica. Con ciò non vogliamo dire che la scelta operata da molti dirigenti scolastici di consentire l'accesso ai PEI solo per presa visione negli uffici di segreteria sia sbagliata. La scelta delle procedure da adottare compete infatti al titolare del trattamento che, valutato il contesto specifico, può decidere di proibire la circolazione di documenti in formato digitale per garantire la massima riservatezza delle informazioni in esse contenute. Questa scelta può essere fatta a seguito della valutazione della possibilità di adottare le tecniche di pseudonimizzazione e di cifratura presentate più avanti, della natura dei documenti trattati e della effettiva necessità di costante condivisione fra i componenti del consiglio di classe.

E' però importante capire che la normativa vigente non proibisce l'utilizzo del registro elettronico per la condivisione fra soggetti autorizzati di documenti contenenti dati particolari, a condizione che la scuola definisca procedure che contengano il rischio legato all'errore umano, che nessuna configurazione può escludere del tutto. L'art. 32 del GDPR indica espressamente, fra le misure tecniche adeguate, la

pseudonimizzazione e la cifratura dei dati personali: sono queste le due tecniche che proponiamo, da utilizzare in alternativa o in combinazione fra loro.

5.1 La pseudonimizzazione

La pseudonimizzazione consiste nel trattare i dati in modo che non possano più essere attribuiti a un interessato specifico senza l'utilizzo di informazioni aggiuntive, conservate separatamente e protette da misure adeguate (art. 4, n. 5, del GDPR). In ambito scolastico si realizza associando a ciascun alunno un **codice identificativo**, destinato a sostituire il nome nei documenti riservati.

È un'operazione che la segreteria può compiere a inizio anno scolastico per ciascun alunno, attribuendo codici che non siano ricavabili dal nome, dalla data di nascita o dal numero di registro e riportando l'associazione fra codice e alunno in una tabella da conservare in forma riservata, accessibile al solo personale autorizzato. Il codice attribuito al singolo alunno viene poi comunicato ai docenti della classe alla quale l'alunno è assegnato, che a loro volta dovranno conservare tale informazione in forma riservata. La procedura consente al coordinatore di classe o al docente di sostegno di elaborare documenti pseudonimizzati, nei quali non compaiono il nome, il codice fiscale, la data di nascita o altri dati identificativi dell'alunno, ma soltanto il codice. Se per qualche motivo il documento pseudonimizzato giunge a terzi non autorizzati, ad esempio ai genitori della classe per un errore nel caricamento, esso non è direttamente riconducibile a uno specifico alunno.

La pseudonimizzazione ha però un limite, che va tenuto ben presente: i dati pseudonimizzati restano dati personali, e non impediscono di risalire alla persona cui il documento si riferisce in contesti circoscritti come quello di una classe, nella quale la presenza di alunni con specifiche difficoltà è limitata, al massimo, a poche unità. Il contenuto di un PEI, anche privo del nome, può rendere l'alunno riconoscibile a chi conosce la classe. È per questo che occorre fare riferimento a un ulteriore strumento, che può essere utilizzato in combinazione con la pseudonimizzazione o in alternativa a essa.

5.2 La cifratura dei documenti

La cifratura (o criptaggio) rende il contenuto di un documento accessibile soltanto a chi è in possesso della chiave di decodifica. Nella sua forma più semplice consiste nell'apposizione di una **password di apertura** sui file contenenti dati particolari oggetto di condivisione sul Registro, utilizzando le funzioni già disponibili nei comuni programmi di videoscrittura e di gestione dei PDF, che impiegano algoritmi di cifratura robusti. Occorre fare attenzione a utilizzare la funzione che cifra il documento con password, e non quella che si limita a impedirne la modifica, la quale lascia il contenuto leggibile a chiunque apra il file.

La password può essere definita all'inizio dell'anno scolastico, preferibilmente nella prima seduta del consiglio di classe, e condivisa da tutti i componenti del consiglio, che dovranno mantenerla riservata. Deve essere sufficientemente lunga e non intuibile (non il nome della scuola, della classe o del plesso) e va sostituita se vi è motivo di ritenere che sia stata conosciuta da persone estranee al consiglio. Quando deve essere condiviso nel Registro un documento riservato, il docente lo cifra prima del caricamento: in questo modo il documento resta inaccessibile ai terzi non autorizzati che dovessero venirne in possesso, come nel caso dell'errore commesso nella scelta dell'area o dei destinatari. Per una maggiore garanzia la cifratura può essere applicata a un documento già pseudonimizzato.

Il beneficio non è soltanto pratico. Una violazione che riguardi dati resi incomprensibili a chi non è autorizzato ad accedervi presenta un rischio sensibilmente minore per gli interessati, e l'art. 34, par. 3, lett. a), del GDPR esclude espressamente, in questo caso, l'obbligo di comunicazione della violazione agli interessati. L'evento andrà comunque segnalato al Dirigente Scolastico e annotato nel registro delle violazioni (art. 33, par. 5, del GDPR), ma le sue conseguenze risulteranno di norma assai più contenute.

La tabella di corrispondenza fra codici e alunni e la password del consiglio di classe sono esse stesse informazioni riservate: non vanno conservate nel Registro, né riportate nei verbali, né trasmesse insieme ai documenti che proteggono. Una password comunicata nello stesso messaggio o nella stessa area in cui si trova il file annulla la misura.

5.3 La nostra indicazione

Il nostro suggerimento è quello di **adottare sempre la cifratura con password definite all'inizio dell'anno scolastico** per tutti i documenti contenenti dati particolari condivisi nel Registro, perché si tratta della procedura più semplice da attuare e al tempo stesso della più efficace nel prevenire le conseguenze di un errore. Ove la scuola sia in grado di gestire procedure più articolate, potrà associare alla cifratura anche la pseudonimizzazione dei documenti da condividere.

Quanto alla trasmissione di questi documenti alle famiglie, la soluzione da preferire resta la consegna diretta al genitore dell'alunno interessato. Ove si utilizzi il Registro, il documento va reso visibile ai soli genitori di quell'alunno, con comunicazione individuale, e protetto con una password diversa da quella del consiglio di classe, comunicata alla famiglia per altra via.

6. Che cosa fare all'avvio dell'anno scolastico

Riassumiamo di seguito gli adempimenti che suggeriamo di completare in concomitanza con l'avvio dell'anno scolastico:

- 1) verificare la configurazione degli accessi: accesso esclusivo con SPID o CIE per il personale, con disattivazione delle credenziali tradizionali, e procedura di rilascio delle credenziali ai genitori impossibilitati, secondo le indicazioni e i modelli della nota [DPO 97/2026](#), che riportiamo di seguito per comodità:
 - [Allegato 1a – Circolare al personale delle scuole che accedono già con SPID e CIE:](#)
 - [Allegato 1b – Circolare al personale per l'introduzione della nuova regola](#)
 - [Allegato 2 – Comunicazione alle famiglie:](#)
 - [Allegato 3a – Modulo richiesta di rilascio delle credenziali - genitore](#)
 - [Allegato 3b – Modulo richiesta di rilascio delle credenziali - studente](#)
- 2) Stabilire e rendere note le regole per l'uso del registro elettronico:
 - [Regolamento di istituto per utilizzo registro elettronico](#)
 - [Circolare autorizzazione uso RE e presentazione regolamento](#): atto con cui il personale è autorizzato all'uso del RE e riceve le istruzioni per il suo impiego
 - [Guida uso registro elettronico studenti scuole I grado](#)
 - [Guida uso registro elettronico studenti scuole II grado](#)
- 3) verificare con il fornitore ed illustrare ai docenti l'articolazione delle aree riservate e le impostazioni di visibilità predefinite;
- 4) definire la password di cifratura di ciascun consiglio di classe e, ove si adotti anche la pseudonimizzazione, affidare alla segreteria l'attribuzione dei codici agli alunni e la tenuta riservata della tabella di corrispondenza;
- 5) Per garantire la correttezza dei trattamenti operati sul registro elettronico verificare la presenza dei documenti citati nella nota [DPO 36/2025](#) e richiamati poi nella istanza di accesso civico generalizzato presentata da una giornalista in questi giorni a diversi istituti scolastici (vedere nota [DPO 103/2026](#)):
 - [Modello DPIA per uso RE](#)
 - [Informativa per l'uso del RE](#) (tenere comunque presente che nei nostri modelli di informativa generale è presente una sezione che illustra sinteticamente i trattamenti operati sul RE)

- Verificare la formalizzazione dell'incarico di responsabile del trattamento al fornitore del registro elettronico.

7. Note collegate e riferimenti

[DPO 97/2026](#) – Registro Elettronico: l'accesso con SPID e CIE all'avvio dell'anno scolastico;

[DPO 17/2026](#) – SPID e CIE per gli studenti minorenni: chiarimenti sull'accesso al Registro Elettronico;

[DPO 6/2026](#) – Le disposizioni per l'uso del registro elettronico;

[DPO 98/2025](#) – Condivisione di dati e documenti nel consiglio di classe;

[DPO 36/2025](#) – Indicazioni operative per l'uso del registro elettronico;

Provvedimenti del Garante:

[Provvedimento del 27 febbraio 2025 \[doc. web n. 10126123\]](#) – pubblicazione del PEI sul registro elettronico.

Note e documenti ministeriali:

[Circolare MIM 4588 dell'8/11/2023](#)

[Nota MIM 4717 del 12/09/2024](#)

[Nota MIM prot. n. 5274 dell'11/07/2024](#)

[Nota MIM 2773 del 4/4/2025](#)

Servizi assistenza e consulenza Vargiu Scuola

Vargiu Scuola assiste oggi quasi duemila scuole all'interno di specifici contratti che includono l'assunzione del ruolo di:

- **Referenti per la Privacy** (inteso quale consulente)
- **Referenti per la Transizione Digitale e l'IA-** per l'attuazione del CAD e dell'IA Act
- **Referenti per la trasparenza** (inteso quale consulente) – per l'attuazione della normativa in materia di trasparenza ed anticorruzione
- **Referenti per l'accessibilità** - per l'attuazione della normativa sull'accessibilità

Una presentazione dei nostri servizi è disponibile al [presente link](#) mentre l'affidamento può essere fatto da **catalogo MEPA** con i seguenti codici prodotto:

- **VS-CONSIA-1A:** servizio di assistenza nel ruolo di referente per l'attuazione della normativa in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD) – durata 1 anno – **canone 600 € + IVA 22%**
- **VS-CONSIA-3A:** servizio di assistenza nel ruolo di referente per l'attuazione della normativa in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD) – durata 3 anni con possibilità di recesso annuale senza motivazione– **canone annuo 500 € + IVA 22%**

Privacy e consulenza normativa

Se la vostra scuola ha in scadenza il proprio **Responsabile Protezione Dati (RPD/DPO)** può prendere in considerazione la [nostra proposta di contratto](#) che prevede, oltre alla **consulenza per l'attuazione della normativa** in materia di trasparenza, accessibilità, lotta alla corruzione, privacy e digitalizzazione (CAD) anche l'assunzione dell'**incarico di RPD/DPO**. Nella versione più avanzata del contratto sono anche inclusi i **servizi di formazione in materia di privacy** attraverso dei webinar rivolti ai docenti (2 ore in tutto) e al personale amministrativo/direttivo (3 ore e mezza in tutto). Per l'affidamento diretto si può far riferimento ai seguenti prodotti a **catalogo MEPA**:

- **VS-RPDIA-1A:** assunzione dell'incarico di Responsabile Protezione Dati (RPD o DPO) e assistenza in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD e AI Act) – durata 1 anno – **canone 1.200,00 € + IVA 22%**
- **VS-RPDIA-3A:** assunzione dell'incarico di Responsabile Protezione Dati (RPD o DPO) e assistenza in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD e AI Act) – durata 3 anni con possibilità di recesso annuale senza motivazione – **canone annuo 1.100,00 € + IVA 22%**
- **VS-RPDIA-FOR-1A:** assunzione dell'incarico di Responsabile Protezione Dati (RPD o DPO) e assistenza in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD e AI Act). Inclusa formazione privacy per docenti (2 ore) e personale amministrativo direttivo (3 ore e mezza) per mezzo di webinar – durata 1 anno – **canone 1.350,00 € + IVA 22%**
- **VS-RPDIA-FOR-3A:** assunzione dell'incarico di Responsabile Protezione Dati (RPD o DPO) e assistenza in materia di trasparenza, accessibilità, lotta alla corruzione e digitalizzazione delle PA (CAD e AI Act). Inclusa formazione privacy per docenti (2 ore) e personale amministrativo direttivo (3 ore e mezza) per mezzo di webinar – durata 3 anni con possibilità di recesso annuale senza motivazione – **canone annuo 1.250,00 € + IVA 22%**

Si evidenzia che la durata pluriennale del contratto è suggerita da ANAC con la [delibera 13 maggio 2020](#) e da una successiva comunicazione del Garante privacy in modo da garantire la stabilità di una figura di grande rilievo che necessita, per il suo operato, di continuità nel tempo.

La sintesi delle nostre proposte

Codice contratto	Assistenza privacy, trasparenza, accessibilità, lotta alla corruzione e digitalizzazione	Incarico RPD	Formazione docenti (webinar 2 ore) e personale amministrativo/direttivo (webinar 3 ore e mezza)
VS-CONSIA-1A VS-CONSIA-3A	SI	NO	NO
VS-RPDIA-1A VS-RPDIA-3A	SI	SI	NO
VS-RPDIA-FOR-1A VS-RPDIA-FOR-3A	SI	SI	SI

Le scuole che hanno in scadenza il proprio DPO e che sono interessate ai nostri servizi per l'attuazione della normativa in materia di privacy, trasparenza, accessibilità, lotta alla corruzione e CAD possono ovviamente far riferimento alle nostre proposte **VS-RPDIA-1A e VS-RPDIA-3A** o a quelle **VS-RPDIA-FOR-1A e VS-RPDIA-FOR-3A** che includono anche il servizio di formazione.

Se invece il DPO non ha il contratto in scadenza la scuola può prendere in considerazione le nostre proposte [VS-CONSIA-1A e VS-CONSIA-3A](#) che per il canone annuale di 600,00 € + IVA (contratto annuale) o di 500,00 € + IVA (contratto triennale) consentono di avere un referente per l'attuazione della normativa (ma non un RPD/DPO). Alla scadenza del contratto del vostro DPO potreste quindi prendere in considerazione la proposta Vargiu Scuola per un servizio che include l'assunzione dell'incarico di DPO e di referente normativo (VS-RPDIA-1A e VS-RPDIA-3A). In tal caso si procederebbe alla rescissione del precedente contratto con Vargiu Scuola per il quale verrà addebitato il solo periodo di effettiva prestazione del servizio.

Risorse PNRR (DM 219 e DM 38)

I servizi sopra descritti sono erogati attraverso una piattaforma documentale Alfresco con l'intero corpo documentale e le guide operative per la gestione di privacy, trasparenza, accessibilità, prevenzione della corruzione, digitalizzazione e governo dell'intelligenza artificiale, unitamente al canale di assistenza e consulenza sulle medesime materie. L'uso di una simile piattaforma è finanziabile con risorse PNRR (costi indiretti per il DM 219; software e licenze per piattaforme di content-sharing per il DM 38) nei limiti previsti dagli avvisi.

Abbiamo quindi caricato a catalogo MEPA i codici per l'uso della piattaforma Alfresco e la fruizione dei relativi servizi di assistenza e consulenza (gli stessi, in sostanza, prestati con il codice **VS-CONSIA-1A** sopra riportato) e che riportiamo di seguito:

Codice MEPA	Finanziamento	Costo	Costi Rendicontabili PNRRi
Alfresco-DM219	DM 219/2025	550,00 € + IVA 22%	Costi indiretti erogati fino al 31/12/2026 (accesso gratuito alla piattaforma fino al 31/8/2027)
Alfresco-DM38	DM 38/2026	550,00 € + IVA 22%	software e licenze per piattaforme di content-sharing fino al 30/9/2026 (accesso gratuito alla piattaforma fino al 31/8/2027)

Entrambi i codici sono **riservati esclusivamente alle scuole che NON hanno un contratto di assistenza con Vargiu Scuola** (i servizi erogati sono i medesimi forniti alle scuole in contratto).

L'oggetto della fornitura è la **licenza di accesso alla piattaforma documentale Alfresco**, comprensiva del supporto tecnico-funzionale all'utilizzo della piattaforma e all'applicazione dei contenuti nelle materie sopra indicate. Per il DM 219 si fa particolare riferimento alla governance dell'intelligenza artificiale a scuola in coerenza con il Regolamento (UE) 2024/1689 (AI Act), la Legge 132/2025 e le Linee guida MIM (D.M. 166/2025) anche se i servizi da noi erogati abbraccieranno anche in questo caso tutte le materie già indicate.

I termini di rendicontazione corrispondono alle scadenze fissate dai rispettivi avvisi (31/12/2026 per il DM 219; 30/9/2026 per il DM 38). Per ciascun codice, **a titolo di liberalità commerciale e senza alcun onere aggiuntivo per l'Istituzione scolastica**, Vargiu Scuola consente la prosecuzione gratuita dell'accesso alla piattaforma **fino al 31 agosto 2027**: tale estensione non costituisce oggetto di rendicontazione, non comporta costi diretti o indiretti a carico della scuola e consente di mantenere operativi i servizi per tutto l'anno scolastico 2026/27.

Le scuole interessate possono procedere all'acquisto sul MEPA mediante ODA, Trattativa Diretta o RDO, secondo le procedure ordinariamente adottate. Per ogni informazione, per un confronto sulla compatibilità dell'acquisto con il quadro economico del singolo progetto o per ricevere un preventivo personalizzato: **email:** commerciale@vargiuscuola.it, **telefono:** 070271526 - 070271560