I.C. VIA GUICCIARDINI,8 - Protocollo 0008934/2026 del 05/11/2026

MINISTERO DELL'ISTRUZIONE E DEL MERITO
UFFICIO SCOLASTICO REGIONALE PER IL LAZIO
ISTITUTO COMPRENSIVO VIA GUICCIARDINI 8
Scuola Primaria e Secondaria di I Grado Ruggero Bonghi
Scuola Primaria Alfredo Baccarini
Via Guicciardini, 8 - 00184 Roma –T. 0670453919 F. 06 77079063
Ambito 1 Codice Scuola RMIC817009 Codice Fiscale 97204170589
Peo. rmic817009@istruzione.it Pec. rmic817009@pec.istruzione.it
www.icguicciardiniroma.edu.it

Al sito web della scuola - sezione Privacy
Alle piattaforme e agli atti delle procedure di affidamento
All'albo online e ad Amministrazione trasparente, quando pertinente
Agli atti

INFORMATIVA SUL TRATTAMENTO DEI DATI PERSONALI OPERATORI ECONOMICI, FORNITORI, APPALTATORI E SUBAPPALTATORI E PERSONE FISICHE A ESSI COLLEGATE

ai sensi degli articoli 13 e 14 del Regolamento (UE) 2016/679

A chi è rivolta. Questa informativa riguarda gli operatori economici persone fisiche e le persone fisiche i cui dati sono trattati nell'ambito di consultazioni di mercato, affidamenti, gare e contratti della scuola: titolari di impresa individuale, soci e amministratori, legali rappresentanti, procuratori, titolari effettivi, referenti, firmatari, dipendenti, collaboratori, tecnici, professionisti, garanti e persone collegate a subappaltatori o ausiliarie.

Il Regolamento europeo protegge le persone fisiche. Quando il fornitore è una società o un altro ente, questa informativa non riguarda l'ente in quanto tale, ma i dati personali delle persone che agiscono per suo conto o che sono indicate nella documentazione. La scuola tratta solo i dati necessari per scopi determinati e con misure adeguate di sicurezza.

IN BREVE
A chi si applica? Alle persone fisiche collegate a operatori economici e fornitori: titolari, rappresentanti, titolari effettivi, referenti, dipendenti, collaboratori, tecnici e subappaltatori.
Perché usiamo i dati? Per affidamenti e gare, verifica dei requisiti, stipula ed esecuzione dei contratti, sicurezza, fatture e pagamenti, trasparenza, controlli e tutela dei diritti.
Per quanto tempo? Secondo le norme sui contratti pubblici e il piano di conservazione; i documenti contabili sono conservati di regola almeno dieci anni.
A chi possono essere comunicati? Ai soggetti indicati nell'informativa, comprese le autorità e le piattaforme pubbliche necessarie alla procedura e al contratto.
A chi puoi scrivere? RMIC817009@istruzione.it **RPD/DPO:** microtech@webmicrotech.it
Quali diritti hai? Puoi chiedere accesso e rettifica e, nei casi previsti, cancellazione, limitazione, portabilità o opposizione; puoi presentare reclamo al Garante.
Decisioni e IA. L'aggiudicazione, l'esclusione e le decisioni sul contratto non sono affidate esclusivamente a sistemi automatizzati; gli strumenti di IA autorizzati restano soggetti a verifica umana.
Se tratti dati per la scuola. Gli obblighi sul trattamento dei dati di alunni, famiglie o personale sono regolati separatamente dal contratto e, quando necessario, dall'atto previsto dall'art. 28 GDPR.

Le informazioni complete, comprese le basi giuridiche e le eccezioni, sono riportate nelle sezioni seguenti.

1. Chi decide come vengono usati i dati?



Il Titolare del trattamento, cioè il soggetto che decide perché e come usare i dati, è l'Istituzione scolastica rappresentata dal Dirigente scolastico in carica.

Contatti de Titolare del Trattamento: I.C. Via Guicciardini,8, sita in Via Guicciardini,8 Dirigente Scolastica Simona Di Matteo, tel. 0670453919 e-mail: RMIC817009@istruzione.it pec: RMIC817009@pec.istruzione.it

Per richieste sui dati personali è utile indicare nell'oggetto: "Privacy - esercizio dei diritti".

2. Chi può aiutarti per le questioni sulla privacy?



La scuola ha nominato un Responsabile della protezione dei dati (RPD), chiamato anche Data Protection Officer (DPO). Il RPD può essere contattato per domande sull'uso dei dati e sull'esercizio dei diritti.

Contatti del RPD: dr. Attilio Milli, amministratore della società Microtech s.r.l. e-mail: dpo@gdpristruzione.it

3. Quali dati vengono raccolti e da dove provengono?



La scuola può trattare dati anagrafici e di contatto, codice fiscale, residenza e cittadinanza, qualifica e poteri di rappresentanza, firma autografa o digitale e dati del certificato, curriculum e requisiti professionali, iscrizioni ad albi o registri, dati dell'impresa individuale, partecipazioni e titolarità effettiva, dichiarazioni su conflitti di interessi, dati economici, fiscali, contributivi, assicurativi e bancari, estremi di CIG e CUP, documenti di identità quando necessari e dati tecnici relativi ad account, indirizzo IP, accessi e operazioni sulle piattaforme.

Quando previsto dalla legge possono essere trattati dati relativi a condanne penali, reati, misure di sicurezza, cause di esclusione, interdittive o sanzioni. Categorie particolari di dati sono di regola escluse e sono acquisite solo se indispensabili per sicurezza, obblighi di legge, esercizio o difesa di un diritto, con accessi limitati e garanzie adeguate.

Origine dei dati. I dati possono essere forniti dall'interessato, dall'operatore economico, dall'appaltatore per conto di subappaltatori e ausiliarie o da altri soggetti legittimati. Possono provenire da documenti di gara e contrattuali, altre stazioni appaltanti o amministrazioni, Camera di commercio e registri professionali, ANAC e Fascicolo virtuale dell'operatore economico (FVOE), Banca dati nazionale dei contratti pubblici (BDNCP), DURC online, banche dati fiscali, previdenziali, antimafia e giudiziarie autorizzate, Consip e Mercato elettronico della pubblica amministrazione (MEPA), piattaforme di approvvigionamento digitale, ReGiS, enti finanziatori, autorità e altre fonti pubbliche previste dalla legge.

Quando i dati non sono raccolti direttamente presso l'interessato, questa informativa è resa entro un mese oppure, se avviene prima, al momento della prima comunicazione all'interessato o a un altro destinatario, salvo le eccezioni dell'art. 14 del Regolamento europeo. Il collegamento è inserito nella lettera di invito, richiesta di preventivo, trattativa diretta o ordine su MEPA, nel contratto e nei moduli di autorizzazione all'accesso. Il contratto obbliga l'operatore a consegnarla alle persone i cui dati trasmette e a propagare l'obbligo ai subappaltatori, ferma la responsabilità informativa del Titolare.

Personale a contatto con minori. Quando il servizio comporta contatti diretti e regolari con gli alunni, il fornitore, quale datore di lavoro, richiede per il personale impiegato il certificato penale previsto dall'art. 25-bis del D.P.R. 313/2002. La verifica della scuola si fonda sull'adempimento di obblighi di legge e sull'esecuzione di compiti di interesse pubblico, ai sensi dell'art. 6, par. 1, lett. c) ed e), GDPR e dell'art. 2-ter del D.lgs. 196/2003. Di regola la scuola acquisisce una dichiarazione di avvenuto controllo riferita al personale impiegato e non conserva copia dei certificati. Se una norma o un'autorità richiede l'acquisizione, i dati giudiziari sono trattati ai sensi degli artt. 10 GDPR e 2-octies del D.lgs. 196/2003, con accessi limitati, custodia separata e cancellazione o distruzione al termine della verifica, salvo obblighi ulteriori. Nel caso di esperti esterni o collaboratori diretti

Modalità adottata dall'Istituto per la verifica ex art. 25-bis: Viene acquisita la sola dichiarazione del fornitore.

Conferimento. I dati richiesti dalla legge, dagli atti di procedura o dal contratto devono essere forniti. In mancanza, la scuola può non poter ammettere l'operatore, verificare i requisiti, affidare o eseguire il contratto, autorizzare accessi o effettuare pagamenti. Non viene richiesto il consenso per i trattamenti necessari alla procedura, al contratto o agli obblighi pubblici.

4. Perché vengono usati i dati e per quanto tempo?



La tabella collega ogni scopo alla regola che consente il trattamento, ai dati che richiedono maggiore tutela e al periodo di conservazione. I tempi seguono il piano di conservazione della scuola, il titolario e il Manuale di gestione documentale.

Il decreto legislativo 30 giugno 2003, n. 196, di seguito indicato come D.lgs. 196/2003, contiene il Codice italiano in materia di protezione dei dati personali.

Per quale scopo	Perché il trattamento è consentito	Dati che richiedono maggiore tutela	Per quanto tempo
a) Consultazione del mercato e procedura di affidamento Indagini di mercato, elenchi, richieste di preventivo, manifestazioni di interesse, gare, offerte, soccorso istruttorio e aggiudicazione.	Obblighi di legge e compiti pubblici: art. 6, par. 1, lett. c) ed e), GDPR e art. 2-ter del D.lgs. 196/2003; D.lgs. 36/2023. Per l'operatore persona fisica anche misure precontrattuali: lett. b).	Di regola non richiesti. Se indispensabili e previsti dalla legge: artt. 9 e 10 GDPR, artt. 2-sexies, 2-septies e 2-octies del D.lgs. 196/2003.	Per la durata della procedura. Le offerte non aggiudicate e la documentazione dei concorrenti esclusi sono conservate di regola 5 anni dalla conclusione, salvo contenzioso, controlli o diversi termini del massimario; gli atti del fascicolo seguono le regole archivistiche.

Per quale scopo	Perché il trattamento è consentito	Dati che richiedono maggiore tutela	Per quanto tempo
b) Verifica dei requisiti e dell'integrità **Requisiti generali e speciali, FVOE, DURC, regolarità fiscale, antimafia, conflitti di interessi, sanzioni, titolare effettivo e controlli su dichiarazioni.**	Art. 6, par. 1, lett. c) ed e), GDPR; art. 2-ter del D.lgs. 196/2003; artt. 16, 94-96, 98 e 99 del D.lgs. 36/2023; D.lgs. 159/2011, D.P.R. 313/2002, legge 190/2012, art. 6-bis legge 241/1990, D.P.R. 62/2013 e art. 53, c. 16-ter, D.lgs. 165/2001.	Dati giudiziari nei casi autorizzati: art. 10 GDPR, art. 2-octies del Codice, artt. 94-96 e 98 del D.lgs. 36/2023, D.lgs. 159/2011 e D.P.R. 313/2002. Categorie particolari solo se indispensabili e con le garanzie di legge.	Secondo i termini della procedura, dei controlli e del piano di conservazione; più a lungo in caso di contenzioso, finanziamenti, verifiche o obblighi dell'autorità.
c) Stipula ed esecuzione del contratto **Ordini, consegne, collaudi e verifiche, garanzie, penali, subappalto, accesso ai locali, sicurezza sul lavoro, referenti e personale impiegato.**	Art. 6, par. 1, lett. b), c) ed e), GDPR; art. 2-ter del Codice; artt. 119 e seguenti del D.lgs. 36/2023, art. 26 del D.lgs. 81/2008 e disciplina contrattuale applicabile.	Solo se indispensabili per sicurezza, difesa o obblighi di legge: art. 9, par. 2, lett. b), f) o g), con artt. 2-sexies e 2-septies; art. 10 e art. 2-octies per dati giudiziari.	Per la durata del contratto e per i successivi termini di garanzia, controllo, prescrizione, rendicontazione e conservazione archivistica.
d) Contabilità, fatturazione e pagamenti **Fatture elettroniche, IBAN e conto dedicato, persone delegate, CIG e CUP, tracciabilità dei flussi, verifiche fiscali e contributive, certificazioni e rendicontazione.**	Art. 6, par. 1, lett. b), c) ed e), GDPR; normativa fiscale e contabile, legge 136/2010, D.lgs. 36/2023 e regole sui finanziamenti.	Non previsti in via ordinaria. Eventuali dati giudiziari o particolari sono trattati solo quando una norma lo richiede e nei limiti necessari.	Documentazione fiscale e contabile di regola almeno 10 anni; ulteriore conservazione quando richiesta da controlli, finanziamenti, contenzioso o regole archivistiche.
e) Pubblicità, trasparenza e accesso **Albo, Amministrazione trasparente, BDNCP, dati sul ciclo di vita del contratto, accesso documentale e accesso civico.**	Art. 6, par. 1, lett. c) ed e), GDPR; artt. 28, 35 e 36 del D.lgs. 36/2023; artt. 5, 5-bis e 37 del D.lgs. 33/2013; legge 241/1990 e provvedimenti ANAC applicabili.	Dati particolari e giudiziari non sono pubblicati, salvo espresso obbligo e nei limiti strettamente necessari. Dati non pertinenti sono oscurati.	Per il periodo di pubblicazione previsto dalla legge; gli atti restano conservati secondo il piano, con limitazione dell'indicizzazione quando applicabile.
f) Servizi digitali e sicurezza **Piattaforme di approvvigionamento, identità digitale, firme, comunicazioni, videoriunioni, registrazioni tecniche, assistenza, prevenzione di abusi e incidenti.**	Art. 6, par. 1, lett. b), c) ed e), GDPR; art. 2-ter del Codice; D.lgs. 36/2023 e obblighi di sicurezza e amministrazione digitale.	Non previsti in via ordinaria. Se presenti in documenti o comunicazioni, sono protetti con accessi selettivi e trattati solo in presenza di una valida base giuridica.	Per la durata dell'account o del servizio. Log degli amministratori di sistema almeno 6 mesi; altri log di sicurezza di regola non oltre 180 giorni, salvo incidenti, controlli o obblighi che richiedano ulteriore conservazione.
g) Controlli, segnalazioni e tutela dei diritti **Audit, ispezioni, prevenzione di frodi, contestazioni, recupero crediti, contenzioso, richieste delle autorità e whistleblowing.**	Art. 6, par. 1, lett. c) ed e), GDPR; norme sui controlli pubblici, sulla difesa dei diritti, D.lgs. 24/2023 e disciplina di settore.	Art. 9, par. 2, lett. f) e g), quando necessario; art. 10 GDPR e art. 2-octies del Codice. Il whistleblowing ha informativa specifica e canale separato.	Secondo i termini di prescrizione, impugnazione, difesa e conservazione; segnalazioni non oltre 5 anni dall'esito finale, salvo necessità di tutela.
h) PNRR e altri fondi europei **Monitoraggio, rendicontazione, prevenzione di frodi, corruzione, conflitti di interessi e doppio finanziamento; identificazione del titolare effettivo.**	Art. 6, par. 1, lett. c) ed e), GDPR; art. 2-ter del Codice; art. 22 del Regolamento (UE) 2021/241, D.lgs. 231/2007 e regole del programma di finanziamento.	Nome, cognome, data di nascita e codice fiscale del titolare effettivo; eventuali dati giudiziari solo nei casi autorizzati dall'art. 10 GDPR e dall'art. 2-octies del Codice.	Per i termini stabiliti dal programma e comunque per il periodo necessario a monitoraggio, rendicontazione, controlli e audit; più a lungo in caso di contenzioso o obblighi archivistici.

Riferimenti principali di settore: D.lgs. 36/2023, come modificato; D.lgs. 33/2013; legge 241/1990; legge 136/2010; D.lgs. 81/2008; D.lgs. 159/2011; D.P.R. 313/2002; D.P.R. 445/2000; D.P.R. 62/2013; D.lgs. 165/2001; legge 190/2012; D.lgs. 231/2007; Regolamento (UE) 2021/241; D.lgs. 24/2023; normativa fiscale, contabile, antimafia, anticorruzione, sull'amministrazione digitale, sui finanziamenti e sulla conservazione applicabile.

5. Chi può usare, ricevere o vedere i dati?



Possono usare i dati il Dirigente scolastico e le persone autorizzate in base ai compiti, tra cui DSGA, responsabile unico del progetto (RUP), responsabili di fase e di procedimento, direttore dell'esecuzione, personale amministrativo e tecnico, commissioni e seggi di gara, collaudatori, verificatori e consegnatari. L'accesso è limitato alle informazioni necessarie.

Nei casi previsti i dati possono essere comunicati ad ANAC, Ministeri e uffici scolastici, Consip e centrali di committenza, gestori di piattaforme di approvvigionamento digitale, Agenzia delle entrate e Sistema di interscambio, MEF e Ragioneria generale dello Stato, Banca d'Italia e tesoriere, Camera di commercio, INPS, INAIL e casse previdenziali, Prefettura e autorità antimafia, enti finanziatori e di controllo, revisori dei conti, Corte dei conti, altre stazioni appaltanti, amministrazioni certificanti, assicurazioni e garanti, autorità giudiziaria e di pubblica sicurezza, avvocati e professionisti incaricati. Ciascun destinatario riceve solo i dati necessari e opera secondo il ruolo previsto dalla legge.

Piattaforme e banche dati pubbliche. Ai sensi degli artt. 23 e 24 del D.lgs. 36/2023, BDNCP, Piattaforma contratti pubblici e FVOE sono gestiti da ANAC; Consip gestisce i propri strumenti, compreso il MEPA. Le amministrazioni che determinano finalità e mezzi operano come titolari autonomi. Il gestore della piattaforma certificata scelta dalla scuola, quando tratta dati per suo conto e secondo le sue istruzioni, opera invece come Responsabile del trattamento ai sensi dell'art. 28 GDPR. La scuola alimenta i sistemi per gli obblighi del ciclo di vita digitale del contratto.

Contratti finanziati con risorse europee. Per gli affidamenti PNRR o finanziati da altri programmi europei, la scuola tratta i dati anche per prevenire frodi, corruzione, conflitti di interessi e doppio finanziamento e per identificare il titolare effettivo dell'operatore, dell'appaltatore e del subappaltatore ai sensi dell'art. 22 del Regolamento (UE) 2021/241. Possono essere raccolti nome, cognome, data di nascita e codice fiscale e i dati possono essere inseriti in ReGiS, gestito dal MEF - Ragioneria generale dello Stato, e nelle ulteriori piattaforme di monitoraggio e rendicontazione.

Commissione europea, Ufficio europeo per la lotta antifrode (OLAF), Corte dei conti europea e Procura europea (EPPO) possono accedere ai dati e ai documenti per i controlli previsti dall'art. 22, par. 2, lett. e), del Regolamento (UE) 2021/241. Restano fermi i controlli della Corte dei conti e degli altri organi nazionali. La documentazione è conservata per i termini del programma e per il periodo necessario a controlli e audit.

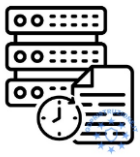
Subappalto. L'autorizzazione e i controlli previsti dall'art. 119 del D.lgs. 36/2023 comportano la verifica dei requisiti del subappaltatore e delle persone rilevanti. I dati possono giungere alla scuola tramite l'appaltatore; l'obbligo di consegnare questa informativa si estende lungo la catena del subappalto e deve essere previsto nei relativi atti.

Trasparenza e pubblicazione. Ai sensi dell'art. 28 del D.lgs. 36/2023, dell'art. 37 del D.lgs. 33/2013 e dei provvedimenti ANAC, i dati del ciclo di vita sono trasmessi alla BDNCP e resi accessibili mediante collegamento in Amministrazione trasparente oppure pubblicati direttamente quando richiesto. La scuola applica pertinenza e minimizzazione e oscura documenti di identità, firme, recapiti personali, coordinate bancarie e informazioni eccedenti. Non è prevista diffusione ulteriore senza un preciso presupposto giuridico.

Accesso agli atti. L'accesso alle procedure e all'esecuzione è disciplinato dagli artt. 35 e 36 del D.lgs. 36/2023 e, per quanto compatibili, dagli artt. 22 e seguenti della legge 241/1990, dal D.P.R. 184/2006 e dagli artt. 5, comma 5, e 5-bis, comma 2, del D.lgs. 33/2013. È assicurato in forma digitale tramite la piattaforma ed è consentito dai momenti stabiliti dall'art. 35; offerte e verbali di valutazione non sono accessibili prima dell'aggiudicazione.

Le informazioni che costituiscono segreti tecnici o commerciali sono sottratte all'accesso quando l'operatore le abbia individuate con dichiarazione motivata e comprovata presentata con l'offerta, fermo l'accesso indispensabile alla difesa in giudizio. Prima dell'ostensione la scuola valuta i controinteressati e oscura i dati personali non pertinenti, compresi documenti di identità, firme, recapiti privati e coordinate bancarie.

6. Come vengono usati i dati nei servizi digitali e con l'intelligenza artificiale?



Le procedure e il contratto possono svolgersi mediante piattaforme di approvvigionamento digitale, PEC, identità digitale, firme elettroniche, fatturazione elettronica e videoriunioni. Possono essere registrati identificativo, account, ruolo, documenti inviati, data e ora, firma e certificato, indirizzo IP, operazioni compiute, esito tecnico e log necessari a sicurezza, tracciabilità e prova della procedura.

Gli account sono personali e non cedibili. La scuola applica autenticazione, profili di accesso, copie di sicurezza, tracciamento degli eventi necessari e controlli sugli accessi. Credenziali smarrite, accessi non autorizzati o errori di trasmissione devono essere segnalati immediatamente. Le videoriunioni non sono registrate, salvo necessità documentata e preventiva informazione specifica.

Decisioni e intelligenza artificiale. La scuola può usare sistemi di IA autorizzati come supporto alla ricerca, alla preparazione o lettura di documenti, alla verifica formale e all'individuazione di anomalie o rischi. L'IA resta strumentale all'attività amministrativa ai sensi dell'art. 14 della legge 132/2025: esclusione, ammissione, valutazione dell'offerta, aggiudicazione, contestazioni e decisioni sul contratto restano affidate a persone competenti e responsabili. La scuola non effettua profilazione né adotta decisioni unicamente automatizzate con effetti giuridici o analogamente significativi nell'ambito dei trattamenti descritti.

Gli operatori non devono inserire dati personali, documenti riservati, segreti tecnici o commerciali, credenziali o atti della procedura in servizi di IA non autorizzati. Se l'impiego di un sistema incide significativamente sulla valutazione di persone o operatori, la scuola svolge le verifiche previste, fornisce un'informazione specifica e assicura intervento umano, possibilità di esprimere osservazioni e contestazione dell'esito. Gli output sono verificati e l'uso è tracciato quando richiesto. L'AI Act è applicato nel testo vigente, come modificato dal Regolamento (UE) 2026/1744.

7. Che cosa accade se il fornitore tratta dati per conto della scuola?



Questa informativa riguarda i dati personali delle persone collegate al fornitore. È distinta dagli obblighi che nascono quando il servizio affidato comporta il trattamento di dati di alunni, famiglie, personale o altri interessati per conto della scuola, ad esempio nei servizi cloud, registro elettronico, assistenza informatica, comunicazione, sicurezza, formazione o sistemi di IA.

Quando ricorrono i presupposti, il fornitore è designato Responsabile del trattamento ai sensi dell'art. 28 del Regolamento europeo mediante contratto o altro atto giuridico. L'atto definisce oggetto, durata, finalità, categorie di dati e interessati, istruzioni documentate, riservatezza, misure di sicurezza, assistenza per diritti e violazioni, cancellazione o restituzione, audit, luoghi del trattamento, trasferimenti e condizioni per i sub-responsabili.

Limiti d'uso. Il fornitore non può usare i dati della scuola per finalità proprie, profilazione, pubblicità, sviluppo o addestramento di modelli di IA, né comunicarli a ulteriori soggetti, salvo espressa previsione lecita e documentata. Non può cambiare luogo di trattamento o ricorrere a sub-responsabili senza rispettare le condizioni contrattuali. Una violazione dei dati o un incidente rilevante deve essere comunicato alla scuola senza ingiustificato ritardo e secondo il termine più breve stabilito nel contratto.

Se il fornitore determina autonomamente finalità e mezzi di uno specifico trattamento, opera invece come titolare autonomo e deve fornire la propria informativa. La qualificazione del ruolo dipende dalle attività effettive e non dal solo nome attribuito nel contratto.

8. Come vengono protetti i dati?



La scuola limita gli accessi in base ai compiti, istruisce il personale, protegge account e dispositivi, aggiorna i sistemi, esegue copie di sicurezza, registra gli eventi necessari e verifica fornitori e piattaforme. I documenti cartacei sono custoditi in ambienti con accesso limitato.

Prima di trattamenti che possono creare un rischio elevato per i diritti e le libertà, la scuola svolge una valutazione d'impatto sulla protezione dei dati. Le misure sono adeguate alla natura del contratto, ai dati accessibili e ai rischi della catena di fornitura. Il fornitore deve rispettare le misure e le istruzioni contenute negli atti di gara, nel contratto e negli allegati di sicurezza.

Personale del fornitore. Per eseguire il contratto la scuola può trattare elenco nominativo, ruolo e qualifica delle persone impiegate dal fornitore e dai subappaltatori, dati di referenti, preposti e addetti alle emergenze, attestati di formazione e abilitazioni, autorizzazioni e sostituzioni. Può verificare i dati esibiti sulla tessera di riconoscimento prevista dall'art. 26, comma 8, del D.lgs. 81/2008, comprendente fotografia, generalità del lavoratore e datore di lavoro, e registrare gli accessi ai locali.

Il trattamento è necessario per la verifica dell'idoneità tecnico-professionale, la cooperazione e il coordinamento, compreso il DUVRI quando previsto, la sicurezza dei luoghi e l'esecuzione del contratto. La scuola non acquisisce giudizi di idoneità alla mansione né documentazione sanitaria del personale del fornitore, che restano presso il datore di lavoro e il medico competente.

Accessi ai locali. Per ingresso, consegna, manutenzione o interventi possono essere registrati identità, impresa, ruolo, orario, area visitata, veicolo e autorizzazione. I registri sono conservati di regola per 6 mesi e poi cancellati, salvo eventi di sicurezza, controlli o contenzioso. Videosorveglianza dell'Istituto: non presente

Consegna dell'informativa. Il contratto obbliga il fornitore a consegnare questa informativa al proprio personale e a quello dei subappaltatori prima dell'avvio. Una copia è allegata al verbale di coordinamento o al DUVRI, quando redatti, ed è resa disponibile con l'autorizzazione di accesso e nella sezione Privacy del sito della scuola.

Segnalazioni di illeciti. Lavoratori, autonomi, collaboratori e professionisti del fornitore possono utilizzare il canale interno della scuola per violazioni apprese nel contesto del rapporto con l'Istituto, quando ricorrono le condizioni del D.lgs. 24/2023, e il canale del proprio datore di lavoro per le violazioni rientranti nel relativo contesto. Resta disponibile il canale esterno ANAC nei casi previsti. Canale interno della scuola e relativa informativa: rmic817009@istruzione.it. L'identità del segnalante è protetta e le segnalazioni sono conservate non oltre cinque anni dall'esito finale, salvo necessità di tutela.

Se una violazione dei dati personali può creare un rischio elevato per le persone, la scuola informa gli interessati senza ingiustificato ritardo, indicando che cosa è accaduto, i possibili effetti e le misure adottate.

9. Quali diritti hai e come puoi esercitarli?



Ai sensi degli artt. 15-22 del Regolamento europeo è possibile chiedere accesso ai dati e rettifica; quando ricorrono le condizioni di legge, cancellazione, limitazione, portabilità oppure opposizione per motivi legati alla propria situazione.

Cancellazione e opposizione non impediscono i trattamenti imposti dalla legge o necessari ai compiti della stazione appaltante. La portabilità si applica solo ai trattamenti automatizzati basati sul consenso o su un contratto e non ai compiti pubblici. Nelle procedure e nei contratti descritti il consenso non costituisce, di regola, la base del trattamento.

L'interessato ha diritto a non essere sottoposto a decisioni unicamente automatizzate che producano effetti giuridici o analogamente significativi, salvo eccezioni e garanzie di legge. Può chiedere informazioni, esprimere osservazioni, contestare la decisione e ottenere un intervento umano. Nei casi previsti dall'art. 86 dell'AI Act può ottenere spiegazioni sul ruolo di un sistema di IA ad alto rischio nella decisione che lo riguarda.

La scuola risponde senza ingiustificato ritardo e comunque entro un mese. Per richieste complesse o numerose il termine può essere prorogato fino ad altri due mesi, informando l'interessato entro il primo mese. L'esercizio dei diritti è gratuito, salvo richieste manifestamente infondate o eccessive.

Nei casi e per il tempo strettamente necessari, l'esercizio dei diritti può essere limitato ai sensi degli artt. 2-undecies e 2-duodecies del D.lgs. 196/2003 quando possa derivarne un pregiudizio effettivo e concreto, tra l'altro, ad attività di controllo o ispezione o alla difesa in giudizio. In tali casi l'interessato è informato nei limiti consentiti e può esercitare i diritti tramite il Garante.

È possibile presentare reclamo al Garante per la protezione dei dati personali: Piazza Venezia 11, 00187 Roma; e-mail protocollo@gpdp.it; PEC protocollo@pec.gpdp.it; sito www.garanteprivacy.it. Resta possibile rivolgersi all'autorità giudiziaria ai sensi dell'art. 79 del Regolamento europeo e dell'art. 152 del D.lgs. 196/2003. Prima del reclamo è possibile contattare la scuola o il RPD.

10. I dati possono essere trasferiti fuori dall'Europa?



Alcuni gestori di piattaforme o servizi digitali possono trattare o rendere accessibili dati fuori dallo Spazio economico europeo. Prima di usare il servizio, la scuola verifica luoghi di trattamento, sub-responsabili e garanzie applicabili.

Il trasferimento è consentito in presenza di una decisione di adeguatezza della Commissione europea oppure di garanzie adeguate, come clausole contrattuali standard e, quando necessarie, misure aggiuntive. Per gli Stati Uniti il Quadro UE-USA sulla protezione dei dati può essere utilizzato solo se il destinatario è certificato e il trattamento rientra nella certificazione. È possibile chiedere informazioni e copia delle garanzie alla scuola o al RPD.

Servizi che comportano accesso o trasferimento extra-SEE:

Servizi: google workspace, Paesi: U.S.A., garanzia applicabile: clausole contrattuali standard.

Se la scuola intende trattare dati già raccolti per una finalità ulteriore rispetto a quella per cui sono stati raccolti, prima del nuovo trattamento fornisce le informazioni sulla diversa finalità e ogni elemento pertinente ai sensi dell'art. 13, par. 3, del Regolamento europeo. La liceità e la compatibilità dell'ulteriore trattamento sono valutate separatamente.

DOCUMENTI COLLEGATI E AGGIORNAMENTI

Questa informativa va letta insieme agli atti della procedura e del contratto, alle informative delle piattaforme e banche dati pubbliche, all'eventuale atto di designazione a Responsabile del trattamento, alle istruzioni di sicurezza e accesso, alle informative su videosorveglianza e whistleblowing e agli atti di valutazione e adozione dei servizi digitali o di IA.

La scuola può aggiornare questa informativa quando cambiano norme, organizzazione, trattamenti, piattaforme o strumenti. La versione aggiornata è pubblicata attraverso i canali istituzionali e richiamata negli atti successivi.

La Dirigente scolastica
Simona Di Matteo
Documento sottoscritto digitalmente

Il 06/11/2026 alle 11:32:07, Simona Di Matteo ha confermato la volonta' di apporre qui la propria Firma Elettronica Avanzata ai sensi dell'art. 20, comma 1-bis del CAD.