

LA RESPONSABILITÀ DEL PERSONALE SCOLASTICO NELLA GESTIONE DEI DATI PERSONALI



OBBLIGHI, PRECAUZIONI E BEST PRACTICE

ISTITUTO COMPRENSIVO CASTELL'ALFERO
21 ottobre 2025

Dott. Gianluca Apicella Fiorentino

Avv. Alessandra Lezzi

EduConsulting



Edu Consulting è una **società** di **consulenza** e **formazione** che opera nel settore Education dal 2018.



Un **team** di giuristi, avvocati ed esperti in appalti e amministrazione scolastica che garantisce la **migliore assistenza**, offrendo **soluzioni su misura** e altamente **specializzate**.



La **mission** è supportare gli Istituti Scolastici nella **complessa gestione delle attività** e degli **adempimenti amministrativi** che gravano su Dirigenti Scolastici e DSGA.

I NOSTRI PUNTI DI FORZA



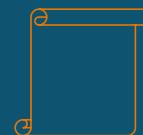
✓RedigoPA



**CONCESSIONI, DISTRIBUTORI
AUTOMATICI E SERVIZIO BAR**



SUPPORTO E CONSULENZA



GARE SOPRA SOGLIA



**DPO, PRIVACY e
AMMINISTRAZIONE TRASPARENTE**



FORMAZIONE AL PERSONALE

FONTI E RIFERIMENTI NORMATIVI

**IL GARANTE DELLA PRIVACY
AGGIORNA PERIODICAMENTE LE
FAQ "SCUOLA E PRIVACY"
CONSULTABILI AL SEGUENTE LINK**



<https://www.garanteprivacy.it/home/faq/scuola-e-privacy>
<https://www.gpdp.it/podcast>

**La scuola a prova di privacy
Vademecum ed. 2023.pdf**



<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9886884>



Sciagurati!

GDPR 2016/679: cos'è?

GDPR (General Data Protection Regulation) in italiano RGD (Regolamento Generale sulla Protezione dei Dati):

↳ È un **regolamento** attraverso il quale la **Commissione Europea** ha inteso rafforzare la **protezione dei dati personali** dei cittadini dell'Unione Europea. Il Regolamento a differenza delle direttive (che sono recepite con norme interne dagli Stati membri) è direttamente applicabile all'interno degli Stati membri.

↳ Si applica alle **persone fisiche**, a prescindere dalla nazionalità o dal luogo di residenza, in relazione al trattamento dei loro dati personali (**persone giuridiche? Trattamento personale o domestico? Dati anonimi?**)

↳ Deve essere rispettato da tutte le **aziende pubbliche** e **private** nonché dalle **Pubbliche Amministrazioni** con sede nell'Unione Europea e dalle aziende con sede fuori UE che elaborano e trattano dati dei cittadini di uno degli Stati membri (p.e. si pensi alle società che offrono beni o servizi agli interessati in uno o più Stati membri dell'Unione e che effettuano un monitoraggio del comportamento degli interessati attraverso tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali. C.23 e 24 GDPR)

↳ Si applica a qualsiasi **trattamento automatizzato e non** (p.e dati contenuti in un archivio) di **dati personali**

ENTRATA IN VIGORE E APPLICAZIONE

- ☒ Il Regolamento UE 2016/679 è entrato in vigore il **24 maggio 2016**
- ☒ Ha visto applicazione in via diretta in tutti i paesi UE a partire dal **25 maggio 2018**
- ☒ Ha abrogato la direttiva privacy EU 95/46
- ☒ In Italia, il **D. Lgs. 101/2018** del 10 Agosto che è entrato in vigore il **19 Settembre 2018** ha adeguato e modificato il D. lgs. 196/2003 (Codice della Privacy) alle disposizioni del prevalente UE (GDPR).
- ☒ Le disposizioni nazionali devono, comunque, essere interpretate ed applicate alla luce di quanto prescritto dal Regolamento Ue 2016/679 in materia di protezione dei dati personali (art. 288 TFUE)

D. LGS. 101/2018: cos'è?

- ☐ **Art. 13 Legge di delegazione europea** 25 ottobre 2017 n.163 per la modifica del Codice privacy
- ☐ Ha **abrogato** numerose disposizioni del **D.LGS n. 196/2003** non compatibili con il Regolamento
- ☐ Ha introdotto **nuove disposizioni** all'interno del **D.LGS n. 196/2003**
- ☐ Ha **eliminato** alcune **sanzioni penali**: «ne bis in idem» (p.e. Eliminazione del reato di cui all'art. 169 del previgente Codice, "Misure di sicurezza")
- ☐ Inasprimento dell'impianto sanzionatorio con **sanzioni amministrative** (sanzioni fino a 10 milioni di euro nel caso di mancata designazione del DPO- sanzioni fino a 20 milioni di euro per inosservanza dei principi base del trattamento), **penali** (p.e. le sanzioni penali prevedono la reclusione fino a sei anni nel caso di comunicazione o diffusione illecita di dati personali oggetto di trattamento su larga scala) **e civili** (risarcimento del danno materiale o immateriale)
- ☐ Attribuzione di maggiori poteri all' **Autorità di controllo nazionale**

D. L. 8 ottobre 2021, n. 139

Disposizioni urgenti per l'accesso **alle attività culturali, sportive e ricreative**, nonché per **l'organizzazione di pubbliche amministrazioni** e in materia di **protezione dei dati personali**.

- Ha introdotto disposizioni in materia di protezione dei dati personali
- All'articolo 2-ter dopo il comma 1 e' inserito il seguente:

"1-bis Il trattamento dei dati personali da parte di un'amministrazione pubblica di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, **e' anche consentito se necessario per l'adempimento di un compito svolto nel pubblico interesse o per l'esercizio di pubblici poteri ad esse attribuiti.**

La finalità' del trattamento, **se non espressamente prevista da una norma di legge o di regolamento, e' indicata dall'amministrazione, in coerenza al compito svolto o al potere esercitato**, assicurando adeguata pubblicità' all'identità' del titolare del trattamento, alle finalità' del trattamento e fornendo ogni altra informazione necessaria ad assicurare un trattamento corretto e trasparente con riguardo ai soggetti interessati e ai loro diritti di ottenere conferma e comunicazione di un trattamento di dati personali che li riguardano.";

LA PROTEZIONE DEI DATI PERSONALI

PERCHÉ È INDISPENSABILE

- ☒ Garantisce la **veridicità** e **affidabilità** dei dati utilizzati. Essa rappresenta una condizione **indispensabile** per garantire la **riservatezza**, la **libertà** di **autodeterminazione**.
- ☒ Nasce come risposta alla rapidità **dell'evoluzione tecnologica**.
- ☒ Rinunciare alla protezione dei dati personali significa **perdere ogni forma di libertà**.

COSA È UN DATO PERSONALE

- ☒ **Qualsiasi informazione** riguardante una persona fisica identificata o identificabile («interessato»).

- ☒ Si considera identificabile la **persona fisica** che può essere **identificata, direttamente o indirettamente**, con particolare riferimento a:
 - un identificativo anagrafico (nome)
 - un numero di identificazione (codice fiscale)
 - dati relativi all'ubicazione (residenza/domicilio)
 - dato di contatto (numeri telefonici)
 - un identificativo online (e-mail o pec)
 - uno o più elementi caratteristici della sua identità fisica (fisionomia)
 - caratteristiche psichica (carattere o patologia)
 - economica, culturale o sociale.

(art. 4, paragrafo 1)

DATI COMUNI-IDENTIFICATIVI

- ☒ **di persone fisiche:** nome e cognome, indirizzo, residenza anagrafica, numero telefonico, pec, mail, codice fiscale, partita iva ecc. e comunque i dati pubblici in genere.
- ☒ **di enti (sia pubblici che privati), associazioni e società:** sede legale, indirizzo, numero di telefono ecc. NON si dovrebbe applicare il regolamento (C.14 GDPR), però quando si trattano le fatture di persone giuridiche si hanno come riferimento dei dati di contatto di persone fisiche della società/azienda come la mail o tel., quindi si applica il regolamento europeo.

DATI PARTICOLARI

- ☒ **Ex Dati sensibili** (ART. 9 GDPR): dati che rivelino l'origine razziale o etnica, opinioni politiche, convinzioni religiose/filosofiche, appartenenza sindacale, orientamento sessuale, relativi alla salute.
- ☒ **Dati genetici** (C34 GDPR): sono relativi alle caratteristiche genetiche, ereditarie o acquisite, di una persona fisica che forniscono informazioni univoche sulla fisiologia o sulla salute di detta persona fisica (esami DNA, RNA).
- ☒ **Dati biometrici** (C51 GDPR): sono ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici.
- ☒ **Dati giudiziari** (ART. 10 GDPR): possono rivelare l'esistenza di determinati provvedimenti giudiziari penali (ad esempio, i provvedimenti penali di condanna definitivi, la liberazione condizionale, il divieto od obbligo di soggiorno, le misure alternative alla detenzione) o la qualità di imputato o di indagato.

DATI PARTICOLARI

☒ **Art.9 GDPR.**

Divieto di trattamento di dati personali “che rivelino l’origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l’appartenenza sindacale, nonché trattare dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all’orientamento sessuale della persona.”

Il divieto è derogabile in presenza di una delle condizioni:

- **consenso esplicito**
- trattamenti dati nel rapporto di lavoro (Serv. San. per visite fiscali o organi preposti alla vigilanza igienico-sanitaria)
- trattamento è necessario per accertare, esercitare o difendere un diritto in sede giudiziaria
- **trattamento è necessario per motivi di interesse pubblico rilevante sulla base del diritto dell'Unione o degli Stati membri** (art 9, paragrafo 1 e paragrafo 2, lett. g) GDPR; art. 2 sexies novellato D.LGS 196/2003)
- dati personali resi manifestamente pubblici dall’interessato
- il trattamento è necessario per finalità di medicina preventiva o di medicina del lavoro ecc.

DATI PARTICOLARI 1/2

ORIGINI RAZZIALI ED ETNICHE:

I dati che rivelino le origini razziali ed etniche possono essere trattati dalla scuola per favorire l'integrazione degli alunni stranieri. Tali informazioni possono essere in alcuni casi desumibili anche dai nominativi o dai dati anagrafici degli alunni.

CONVINZIONI RELIGIOSE:

Gli istituti scolastici possono utilizzare i dati che rivelino le convinzioni religiose al fine di garantire la libertà di culto e per la fruizione dell'insegnamento della religione cattolica o delle attività alternative a tale insegnamento.

STATO DI SALUTE:

I dati relativi alla salute possono essere trattati per l'adozione di specifiche misure di sostegno o strumenti di ausilio per gli alunni con disabilità, con disturbi specifici di apprendimento o con Bisogni Educativi Speciali; per la gestione delle assenze per malattia; per l'insegnamento domiciliare e ospedaliero a favore degli alunni affetti da gravi patologie; per la partecipazione alle attività sportive, alle visite guidate e ai viaggi di istruzione; in presenza di un regime alimentare differenziato dovuto a intolleranze, allergie o specifiche patologie.

VADEMECUM GARANTE PRIVACY (agg. 2023)

DATI PARTICOLARI 2/2

OPINIONI POLITICHE:

Le opinioni politiche possono essere trattate dalla scuola esclusivamente per garantire la costituzione e il funzionamento degli organismi di rappresentanza: ad es., le consulte e le associazioni degli studenti e dei genitori.

DATI PERSONALI RELATIVI A CONDANNE PENALI E REATI:

I dati personali relativi a condanne penali e reati possono essere trattati per assicurare il diritto allo studio anche a soggetti sottoposti a regime di detenzione o di protezione, come i testimoni di giustizia

VADEMECUM GARANTE PRIVACY (agg. 2023)

TRATTAMENTO DATI: cos'è?

Qualsiasi operazione fatta **su un dato** o su **un insieme di dati personali**, compiuta **con** o **senza l'ausilio** di **processi automatizzati** (art. 4 GDPR)

Alcuni esempi di trattamenti:

- ☒ Raccolta dati (raccogliere dati dall'interessato)
- ☒ Conservazione dei dati (tenuti in archivio)
- ☒ Adattamento dei dati (modifica dei dati)
- ☒ Raffronto dei dati (confronto dati diversi raccolti da più fonti)
- ☒ Messa a disposizione dei dati (metterli a favore di terzi autorizzati)
- ☒ Estrazione dei dati (tirar fuori)
- ☒ Cancellazione o distruzione dei dati (non più disponibili a terzi)

I DATI PERSONALI A SCUOLA

- ☒ Disabilità e DSA
- ☒ Voti ed esami
- ☒ Il registro elettronico
- ☒ Comunicazioni scuola-famiglia
- ☒ Cellulari, foto e video
- ☒ Situazione genitoriale
- ☒ Scuolabus e Mensa Scolastica
- ☒ Videosorveglianza
- ☒ Sportello Psicologico
- ☒ Graduatorie del personale e supplenze
- ☒ Documento del 15 maggio

IL CASO

❓ ISCRIZIONE A SCUOLE E ASILI:

Tutti gli istituti di ogni ordine e grado ma anche gli enti locali eventualmente competenti devono prestare particolare attenzione alle informazioni che richiedono ai fini dell'iscrizione scolastica (effettuata, ad es., attraverso il sistema di iscrizioni online predisposto dal Ministero oppure attraverso moduli cartacei)

Non è possibile richiedere informazioni personali non pertinenti rispetto alla finalità di iscrizione (ad es. lo stato di salute dei nonni o la professione dei genitori).

Particolare attenzione deve essere prestata inoltre all'eventuale raccolta delle categorie particolari di dati personali.

Il trattamento di questi dati, oltre a dover essere espressamente previsto dalla normativa di settore, richiede infatti specifiche garanzie a tutela dei diritti degli interessati e della integrità e riservatezza dei dati (vedi nota del Ministero dell'Istruzione e del merito del 30 novembre 2022).

IL CASO

❓ GESTIONE DEL SERVIZIO MENSA:

Gli enti locali che offrono il servizio mensa possono trattare i dati particolari degli alunni indispensabili per la fornitura di pasti nel caso in cui debbano rispondere a particolari richieste delle famiglie legate, ad es., a determinati precetti religiosi o a specifiche condizioni di salute. Alcune particolari scelte, infatti (pasti vegetariani o rispondenti a determinati dettami religiosi) possono essere idonee a rivelare le convinzioni (religiose, filosofiche o di altro genere) dei genitori e degli alunni.

IL CASO

QUESTIONARI PER ATTIVITÀ DI RICERCA

La raccolta di informazioni personali, spesso anche appartenenti alle particolari categorie di dati, per attività di ricerca effettuate da soggetti legittimati, esterni alla scuola attraverso questionari, è consentita soltanto se i ragazzi, o i genitori nel caso di minori, sono stati preventivamente informati in merito alle caratteristiche essenziali del trattamento dei loro dati personali. Studenti e genitori devono comunque essere lasciati liberi di non aderire all'iniziativa.

IL CASO

❓ **DISABILITÀ E DSA:**

- o sono dati particolari, mai oggetto di diffusione
- o Le scuole possono trattare le categorie particolari di dati personali (es. dati sulle convinzioni religiose, dati sulla salute) solo se espressamente previsto da norme di legge o regolamentari.
- o In ogni caso non possono essere diffusi i dati relativi alla salute: non è consentito, ad esempio, pubblicare online una circolare contenente i nomi degli studenti con disabilità oppure i nomi degli alunni che seguono un regime alimentare differenziato per motivi di salute.

Chi può trattare i dati degli alunni con disabilità?

La conoscenza di tali dati è limitata ai soli **soggetti a ciò legittimati** dalla normativa scolastica e da quella specifica di settore, come ad esempio i docenti, i genitori e gli operatori sanitari che congiuntamente devono predisporre il piano educativo individualizzato (L. n. 104/92, L. n. 328/2000 e D.Lgs. n. 66/2017).

IL CASO: SPORTELLLO ASCOLTO

📌 SPORTELLLO ASCOLTO PSICOLOGICO

Il professionista assume il ruolo di:

- a) **Titolare del trattamento** dei dati personali e particolari degli studenti quando svolge l'attività di natura psicologica in conformità all'articolo 1 della Legge 18 febbraio 1989, n.56 Pertanto lo psicologo anche se esercente una professione sanitaria soggetta al segreto professionale è tenuto a rilasciare adeguata **informativa** e ad acquisire il **consenso** prima di iniziare l'attività di sportello di ascolto.
- b) **Responsabile esterno del trattamento dei dati** quando ha accesso ai dati personali e particolari per conto della Scuola (Titolare del trattamento). Si pensi, ad esempio, al caso in cui la scuola trasferisca allo psicologo l'elenco degli alunni o del personale necessari per l'esecuzione del contratto.

IL CASO: VOTI E SCRUTINI

I voti dei compiti in classe, delle interrogazioni e gli esiti degli esami sono **pubblici**.

Le informazioni sul **rendimento scolastico** sono soggette a un regime di trasparenza e il regime della loro conoscibilità è stabilito dal Ministero dell'istruzione: **sono dati comuni e non particolari**.

ATTENZIONE: Evitare di fornire, anche indirettamente, informazioni sulle condizioni di salute degli studenti: il riferimento alle “prove differenziate” sostenute dagli studenti portatori di handicap, ad esempio, non va inserito nei tabelloni.

ESITI VOTI SCRUTINI FINALI: dove pubblicarli? Pubblicazione nella bacheca fisica della scuola, registro elettronico oppure online?

VOTI E SCRUTINI: PUBBLICAZIONE ONLINE?

Vd. Nota del Garante della Privacy dell'11/06/2020

Pubblicazione dei voti online è **invasiva** e **non coerente** con la più recente normativa sulla privacy.

Per questo il Garante è d'accordo, con la linea del Miur di indicare **l'ammissione degli studenti soltanto sul registro elettronico.**

Spiega il Garante: «Una volta esposti, infatti, i voti rischiano di rimanere in rete per un tempo indefinito e possono essere, da chiunque, anche estraneo all'ambito scolastico, e per qualsiasi fine, registrati, utilizzati, incrociati con altri dati presenti sul web, determinando in questo modo una ingiustificata violazione del diritto alla riservatezza degli studenti, che sono in gran parte minori, con possibili ripercussioni anche sullo sviluppo della loro personalità, in particolare per quelli di loro che abbiano ricevuto giudizi negativi»

IL CASO: ESITO ESAMI DI STATO

- ↯ L'art. 96, comma 2, del decreto legislativo 30 giugno 2003, n. 196, rubricato «Trattamento dei dati relativi agli studenti», stabilisce che *«restano ferme le vigenti disposizioni in materia di pubblicazione dell'esito degli esami mediante affissione all'albo dell'Istituto e di rilascio di diplomi e certificati»*
- ↯ L'art. 3, comma 9, D.P.R. n. 122 del 22 giugno 2009, Regolamento recante coordinamento delle norme vigenti per la valutazione degli alunni e ulteriori modalità applicative in materia precisa che *«gli esiti finali degli esami sono resi pubblici mediante affissione all'albo della scuola, ai sensi dell'articolo 96, comma 2, del decreto legislativo 30 giugno 2003, n. 196»*
- ↯ *La legge del 18 giugno 2009 n. 69, all'art 32 ha disposto che «a far data dal 1° gennaio 2010 gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale si intendono assolti con la pubblicazione sui propri siti informatici da parte delle amministrazioni e degli enti pubblici obbligati».* Era tuttavia garantita l'efficacia legale della pubblicazione a mezzo degli spazi e forme tradizionali dell'Albo pretorio sino al 31 dicembre 2010. A partire invece dal **1° gennaio 2011** le pubblicità effettuate in forma cartacea non hanno effetto di pubblicità legale, di fatto riconoscendo tale caratteristica solo alle affissioni telematiche (comma 5 dello stesso art. 32)

ESAMI DI STATO: COMUNICAZIONE O DIFFUSIONE

COMUNICAZIONE O DIFFUSIONE DI DATI RELATIVI AGLI ESITI FORMATIVI INTERMEDI E FINALI DEGLI STUDENTI (ORIENTAMENTO): richiesta dell'interessato (novellato art. 96 D.LGS 196/2003).

Resta fermo che l'attività di orientamento possa essere svolta dagli istituti anche senza disporre degli elenchi ma con altre modalità ad esempio attraverso la **distribuzione e consultazione di materiale informativo presso le scuole**. (relazione 2007, pag. 47).

Prima di adempiere alla richiesta, gli istituti scolastici devono comunque provvedere a informare **gli studenti su quali dati saranno utilizzati per tali finalità**.

- Un Istituto scolastico comunica i dati personali ad un centro commerciale che vende articoli sportivi al fine di inviare materiale pubblicitario a casa degli studenti (divieto di comunicazione)
- Trasmissione diagnosi funzionale ai fini della determinazione di diritto dell'organico

IL CASO: REGISTRO ELETTRONICO

E' importante tutelare i dati personali degli alunni e dei genitori, visibili ai docenti della classe e via web in alcune piattaforme accessibili anche dalla propria abitazione. Poiché il trattamento dei dati avviene in outsourcing, il Titolare dovrà designare il gestore del Registro quale Responsabile del trattamento.

Le funzionalità del registro elettronico, adeguatamente configurate, possono consentire:

- la condivisione di materiali didattici
- la realizzazione e consultazione di webinar o videolezioni e il dialogo in modo "social" tra docenti, studenti e famiglie, limitando il ricorso a piattaforme che offrono anche molteplici ulteriori servizi, non sempre specificamente rivolti alla didattica

IL CASO: COMUNICAZIONI SCUOLA-FAMIGLIA

**Nelle comunicazioni non dirette a specifici destinatari:
evitare dati personali
(es. vicende di bullismo)**

In particolare, il Garante della privacy precisa che nelle delibere o in altre comunicazioni non rivolte a specifici destinatari non possono essere inseriti dati personali che rendano identificabili gli alunni (ad esempio, quelli coinvolti in casi di bullismo o quelli cui siano state comminate sanzioni disciplinari o interessati da altre vicende delicate).

IL CASO: CELLULARI, FOTO E VIDEO

CIRCOLARE n. 5274 del 11.07.2024, contenente disposizioni sull'uso del dispositivo cellulare nel primo ciclo di istruzione

La circolare suindicata introduce il **divieto di utilizzo in classe del telefono cellulare, anche ai fini educativi e didattici, per gli alunni dalla scuola d'infanzia alla secondaria di primo grado,** salvo i casi in cui lo stesso sia previsto dal PEI O PDP, come strumento di supporto per gli alunni con disabilità o con disturbi specifici di apprendimento ovvero per documentate e oggettive condizioni personali.

Potranno, invece, essere utilizzati per fini didattici altri dispositivi digitali, quali pc e tablet, sotto la guida dei docenti.

IL CASO: CELLULARI, FOTO E VIDEO

- ❖ CIRCOLARE n. 5274 del 11.07.2024, contenente disposizioni sull'uso del dispositivo cellulare nel primo ciclo di istruzione

Ad esempio uno studente potrà registrare per fini personali la spiegazione offerta dal professore per migliorare il proprio apprendimento sulla materia e non potrà pubblicare o diffondere tale registrazione, sia essa audio o video, senza il consenso del professore stesso.

NOTA BENE: E' necessario pertanto procedere all'aggiornamento dei propri regolamenti e il patto di corresponsabilità educativa, prevedendo specifiche sanzioni disciplinari per gli alunni che dovessero contravvenire al divieto di utilizzo in classe dello smartphone.

IL CASO: CELLULARI, FOTO E VIDEO

Fermo restando il diritto dello studente alla tutela della riservatezza, la Scuola può trattare le immagini solo per fini istituzionali previa informativa.

- Foto e video possono essere diffusi sul sito istituzionale, sui social network?
- Qual è la base giuridica su cui si fonda tale trattamento?
- Consenso del soggetto interessato o esecuzione di un pubblico interesse?

Quando il trattamento si fonda sul **consenso dell'interessato**, il **Titolare** deve sempre essere **in grado di dimostrare** (articolo 7.1 del Regolamento) che l'interessato ha prestato il proprio consenso), che è valido se:

1. all'interessato è stata resa l'informazione sul trattamento dei dati personali (articoli 13 o 14 del Regolamento);
2. è stato espresso dall'interessato liberamente, in modo inequivocabile e, se il trattamento persegue più finalità, specificamente con riguardo a ciascuna di esse.
3. Il consenso deve essere sempre revocabile.

IL CASO: CELLULARI, FOTO E VIDEO

IL CONSENSO:

(C43) Per assicurare la libertà di prestare il consenso, è opportuno che il consenso non costituisca un valido fondamento giuridico per il trattamento dei dati personali in un caso specifico, qualora esista un **evidente squilibrio tra l'interessato e il titolare del trattamento, specie quando il titolare del trattamento è un'autorità pubblica e ciò rende pertanto improbabile che il consenso sia stato prestato liberamente in tutte le circostanze di tale situazione specifica.**

Si presume che il consenso non sia stato liberamente prestato se non è possibile prestare un consenso separato a distinti trattamenti di dati personali, nonostante sia appropriato nel singolo caso, o se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione.

IL CASO: CELLULARI, FOTO E VIDEO

Il Gruppo di lavoro Articolo 29 sottolinea che sia **improbabile che le autorità pubbliche possano basarsi sul consenso per effettuare il trattamento** in quanto «quando il titolare del trattamento è un'autorità pubblica sussiste spesso un evidente squilibrio di potere nella relazione tra il titolare del trattamento e l'interessato. In molti di questi casi è inoltre evidente che l'interessato non dispone di alternative realistiche all'accettazione (dei termini) del trattamento.

Tuttavia, non esclude completamente il consenso quale base giuridica per il trattamento dei dati da parte delle autorità pubbliche che può risultare appropriato in casi specifici.

Ad esempio: Scuola pubblica che chiede agli studenti il consenso ad utilizzare le loro fotografie in una rivista studentesca in formato cartaceo. In tale caso il consenso costituisce una libera scelta a condizione che agli studenti non siano negati l'istruzione o altri servizi e che gli studenti possano rifiutare il consenso senza subire alcun pregiudizio.

IL CASO: CELLULARI, FOTO E VIDEO

II TRATTAMENTO FATTO DA UN PRIVATO:

Nel caso di **trattamento fatto da un privato** (tale è il docente che pubblica la foto sul suo profilo personale) richiede un consenso (liberatoria) specifico e preventivo, reso da parte di ciascun genitore a seguito di informativa altrettanto puntuale.

Durante le gite scolastiche, il mandato loro affidato è infatti quello di accompagnare gli alunni e vigilarli durante il viaggio, non di documentare l'attività sui propri profili personali, né tanto meno di diffondere all'universo mondo dati personali di cui sono venuti in possesso.

IL CASO: CELLULARI, FOTO E VIDEO

Trattamento di immagini senza consenso:

- ❖ **Illecito civile:** nel caso in cui un privato pubblichi una immagine di un minore, senza aver ottenuto il consenso dai genitori, gli stessi possono richiedere al Tribunale la rimozione dell'immagine e/o video all'autore o al gestore.
- ❖ **Azione Risarcitoria:** se la pubblicazione delle immagini ha provocato un danno, anche morale, a chi vi è ritratto, i genitori possono richiederne il risarcimento
- ❖ **Trattamento illecito di dati (ex art.167 D.lgs.196/2003 adeguato al D.lgs.101/2018):** se le immagini sono utilizzate per trarne un vantaggio economico, profitto o di arrecare un danno agli interessati, procedendo in violazione al trattamento lecito di dati personali, se dal fatto deriva un vantaggio o, se il fatto consiste nella comunicazione o diffusione di dati personali, è punito con la reclusione da 6 a 24 mesi.
- ❖ **Reato di diffamazione (ex art. 595 c.p.):** se la pubblicazione dell'immagine o del video offende o venga lesa la reputazione di un soggetto di chi vi è ritratto, si risponde del reato di diffamazione aggravata e si rischia la pena della reclusione da 6 mesi a 3 anni più multa non inferiore a 516€

DOCUMENTO DEL 15 MAGGIO

Indicazioni per la redazione del documento del 15 maggio

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9356521>

Come già evidenziato dal Garante, a fronte di specifici obblighi normativi che impongono la diffusione di atti o documenti amministrativi, le amministrazioni pubbliche prima di mettere a disposizione sui propri siti web istituzionali atti e documenti amministrativi contenenti dati personali, devono verificare che sia espressamente previsto **l'obbligo di pubblicare** anche dati personali, ovvero valutare, caso per caso, se tale diffusione sia effettivamente necessaria rispetto alle finalità sottese alla diffusione del documento (art. 4, comma 1, lett. m, e art. 19, comma 3, del Codice, con riguardo ai dati comuni, nonché artt. 20, 21 e 22, comma 11, con riferimento ai dati sensibili e giudiziari).

Ebbene alla luce dei principi e regole sopra richiamati **non si ha alcuna ragionevole evidenza della necessità di fornire alla commissione esaminatrice dati personali riferiti agli studenti in un documento finalizzato ad orientare tale commissione nella redazione del testo della terza prova che sia il più adeguato possibile agli studenti esaminandi.**

È chiaro, infatti, che il senso del documento sia quello di mettere in evidenza il **percorso didattico e formativo di ciascuna classe, prescindendo dalle peculiarità dei singoli elementi che la compongono.**

Lo stesso dato normativo, nonché le successive indicazioni ministeriali al riguardo, non lasciano margini a un'interpretazione estensiva circa il contenuto del documento tale da comprendere anche riferimenti ai singoli studenti, risultando quindi priva del necessario fondamento normativo la diffusione di un documento così redatto.

ALTRI CASI SPECIFICI:

- ❓ **SITUAZIONE GENITORIALE:** Viene ribadito nella nota del MIUR 2 settembre 2015 n. 5536 il diritto alla bigenitorialità e alla condivisione delle scelte educative da parte dei genitori separati, ad eccezione dell'ipotesi di decadenza della responsabilità genitoriale decisa dal Giudice. (p.e. inoltro delle comunicazioni da parte degli uffici di segreteria di tutte le comunicazioni anche al genitore separato/divorziato/non convivente, sebbene non collocatario dello studente interessato; attribuzione della password per l'accesso al registro elettronico ecc...)
- ❓ **DISABILITÀ E DSA:** sono dati particolari, mai oggetto di diffusione
- ❓ **SCUOLABUS E MENSA:** vietato pubblicare gli elenchi degli utenti o i percorsi; la mensa è una questione di competenza degli enti locali, per lo più: convinzioni religiose e dati sanitari relativi ai regimi alimentari

ALTRI CASI SPECIFICI:

2 PAGAMENTO DEL SERVIZIO MENSA

- Non si può pubblicare sul sito della scuola, o inserire in bacheca, il nome e cognome degli studenti i cui genitori sono in **ritardo nel pagamento della retta o del servizio mensa**; né può essere diffuso l'elenco degli studenti, appartenenti a famiglie con reddito minimo o a fasce deboli, che usufruiscono gratuitamente di tale servizio.
- **Gli avvisi messi on line devono avere carattere generale**, mentre alle singole persone ci si deve rivolgere con comunicazioni di carattere individuale.
- Il gestore del servizio deve inviare alle famiglie i "bollettini" di pagamento in busta chiusa. Eventuali buoni pasto, tra l'altro, non possono avere colori differenziati in relazione alla fascia di reddito di appartenenza delle famiglie degli studenti beneficiari. Queste semplici accortezze evitano che soggetti non legittimati possano venire a conoscenza di informazioni idonee a rivelare la situazione economica delle famiglie dei bambini.

ALTRI CASI SPECIFICI:

☒ SERVIZI DI SCUOLABUS PUBBLICAZIONE ONLINE

- Gli istituti scolastici e gli Enti locali non possono pubblicare online (sito della scuola, profilo social, etc.), in forma accessibile a chiunque, gli elenchi dei bambini che usufruiscono dei servizi di scuolabus, indicando tra l'altro le rispettive fermate di salita-discesa o altre informazioni sul servizio. Tale diffusione di dati personali, che tra l'altro può rendere i minori facile preda di eventuali malintenzionati, non può assolutamente essere effettuata o giustificata semplicemente affermando che si sta procedendo in tal senso solo per garantire la massima trasparenza del procedimento amministrativo.

ALTRI CASI SPECIFICI:

AFFISSIONE ELENCHI ALUNNI ALL'INGRESSO DELL'ISTITUTO:

La diffusione di elenchi contenenti dati personali (quali ad esempio “nomi di minori, date di nascita, indirizzi di residenza, numeri di telefono ...”) determina una **violazione della normativa (data breach)** a tutela dei dati personali quando si realizza:

- a) in contrasto ai **principi** di “liceità, correttezza e trasparenza” e di “minimizzazione dei dati”, in violazione dell’art. 5, par. 1, lett. a) e c), del Regolamento;
- b) in assenza di un idoneo presupposto normativo per la diffusione dei predetti dati personali, in violazione dell’art. 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del Regolamento e dell’art. 2-ter, commi 1 e 3, del Codice;

PROVVEDIMENTO DEL GARANTE

AFFISSIONE ELENCHI ALUNNI ALL'INGRESSO DELL'ISTITUTO:

I nominativi degli studenti distinti per classe possono essere resi noti per le classi prime delle scuole di ogni ordine e grado, tramite apposita comunicazione all'indirizzo e-mail fornito dalla famiglia in fase di iscrizione, mentre per le classi successive, l'elenco degli alunni, può essere reso disponibile nell'area del registro elettronico a cui accedono tutti gli studenti della classe di riferimento.

Secondo una prassi ormai consolidata è consentita la pubblicazione al **tabellone** esposto nella bacheca scolastica dei nominativi degli studenti distinti per classe. Tale modalità di pubblicazione del tabellone dovrebbe essere adottata in via residuale solo qualora l'istituzione scolastica sia sprovvista di registro elettronico o sia impossibilitata ad utilizzare strumenti di comunicazione telematica dei dati.

PROVVEDIMENTO DEL GARANTE

AFFISSIONE ELENCHI ALUNNI ALL'INGRESSO DELL'ISTITUTO:

In tutti i casi gli elenchi relativi alla composizione delle classi, resi disponibili con le modalità sopra indicate, devono contenere i **solì nominativi degli alunni e non devono riportare informazioni relative allo stato di salute degli studenti o altri dati personali non pertinenti** (ad es. luogo e data di nascita, etc.).

PROVVEDIMENTO DEL GARANTE

DATA	ACCADUTO	ELEMENTI VALUTABILI DAL GARANTE AI FINI DEL QUANTUM
02.07.2020	Divulgazione di dati e informazioni personali relativi a minori in assenza di un idoneo presupposto normativo per la diffusione dei predetti dati, ai sensi dell'art. 2-ter, commi 1 e 3, del Codice che invece ammette la predetta possibilità da parte di soggetti pubblici solo quando la diffusione è prevista da una norma di legge o, nei casi previsti dalla legge, di regolamento	Opera svolta dall'agente per eliminare o attenuare le conseguenze della violazione, gravità della violazione, della personalità e delle condizioni economiche del contravventore
PROVVEDIMENTO		SANZIONE AMMINISTRATIVA APPLICABILE
Ordinanza di ingiunzione nei confronti di un I.C.		Artt. 58, par. 2, lett. i), e 83 del Regolamento, nonché dell'art. 166 del Codice.
VIOLAZIONE		SANZIONE AMMINISTRATIVA COMMINATA
5, par. 1, lett. a) e c) del Regolamento; 6, par. 1, lett. c) ed e), par. 2 e par. 3, lett. b), del Regolamento e 2-ter, commi 1 e 3, del Codice		Sanzione amministrativa di euro 2000,00.

ALTRI CASI SPECIFICI:

- ❓ **GRADUATORIE DEL PERSONALE E SUPPLENZE:** sono pubbliche per legge, ma soggette al principio di necessità. Dunque nome, cognome, punteggio e posizione in graduatoria, ma non numeri di telefono e/o indirizzi

PROVVEDIMENTO DEL GARANTE

DATA	ACCADUTO	ELEMENTI VALUTABILI DAL GARANTE AI FINI DEL QUANTUM
31.01.2019	Diffusione sul proprio sito web istituzionale di dati personali idonei a rivelare lo stato di salute degli interessati e informazioni contenute nell'elenco graduatorie d'istituto dei docenti rendendole rinvenibili anche digitando sul motore di ricerca Google il numero di telefono di un qualsiasi docente. Nelle graduatorie risultano riportate alcune sigle alfabetiche tra cui la lettera "S" che, secondo quanto indicato nell'Allegato 6 (codici preferenza) del Decreto del Ministero dell'Istruzione Università e Ricerca del 1 aprile 2014, n. 235, individua la categoria degli "invalidi e mutilati civili	Opera svolta dall'agente per eliminare o attenuare le conseguenze della violazione, gravità della violazione, della personalità e delle condizioni economiche del contravventore
PROVVEDIMENTO		SANZIONE AMMINISTRATIVA APPLICABILE
Ordinanza di ingiunzione nei confronti di un II.I.S.S.		ART 162, COMMA 2 BIS Codice Privacy Sanzione amministrativa del pagamento di una somma da euro 10.000,00 (diecimila) a euro 120.000,00 (centoventimila)
VIOLAZIONE		SANZIONE AMMINISTRATIVA COMMINATA
ART 22, COMMA 8 Codice Privacy (D.LGS 196/2003)		Misura minima di euro 4.000,00 (quattromila) per la violazione dell'art. 22, comma 8, del medesimo Codice, applicata in combinato disposto con l'art. 164-bis, comma 1, del medesimo Codice;

ALTRI CASI SPECIFICI:

- ❓ **SITUAZIONE GENITORIALE:** Viene ribadito nella nota del MIUR 2 settembre 2015 n. 5536 il diritto alla bigenitorialità e alla condivisione delle scelte educative da parte dei genitori separati, ad eccezione dell'ipotesi di decadenza della responsabilità genitoriale decisa dal Giudice. (p.e. inoltro delle comunicazioni da parte degli uffici di segreteria di tutte le comunicazioni anche al genitore separato/divorziato/non convivente, sebbene non collocatario dello studente interessato; attribuzione della password per l'accesso al registro elettronico ecc...)

I DATI E L'INTELLIGENZA ARTIFICIALE: LICEITÀ DEL TRATTAMENTO E CRITERI DI SCELTA

ISTITUTO COMPRENSIVO CASTELL'ALFERO
21 ottobre 2025

Dott. Gianluca Apicella Fiorentino

Avv. Alessandra Lezzi

QUADRO NORMATIVO:

- Regolamento UE sull'IA (AI Act), approvato il 13 giugno 2024 e pubblicato nella Gazzetta Ufficiale dell'Unione Europea il 12 luglio 2024
- Linee guida MIM per l'introduzione dell'Intelligenza Artificiale nelle Istituzioni scolastiche (Decreto Ministeriale n. 166 del 9 agosto 2025, aggiornato il 29.98.2025)
- Check list MIM sulle sperimentazioni di Intelligenza artificiale nella scuola
- Reg. UE 2016/679, relativo alla protezione dei dati delle persone fisiche
- D.Lgs 196/2003, c.d. "Codice Privacy"

AREE DI APPLICAZIONE E VANTAGGI PER CATEGORIA

Destinatario	Vantaggi / Esempi di Applicazione	
Dirigente Scolastico	Supporto alle decisioni strategiche: monitoraggio dei documenti programmatici (PTOF, RAV), pianificazione della formazione, ottimizzazione nella riorganizzazione dell'orario.	Chatbot per smistamento richieste, gestione di comunicazioni/circolari periodiche, gestione dell'inventario
Personale Amministrativo (DSGA/ATA)	Ottimizzazione dei processi routinari.	Personalizzazione dei materiali didattici, creazione di percorsi formativi su misura, supporto alla valutazione formativa.
Studente	Strumenti per l'apprendimento critico: Tutor virtuali per approfondimenti, strumenti di ricerca e analisi.	

REGOLAMENTO UE SULL'IA (AI Act)

Il Regolamento è entrato in vigore il 1° agosto 2024, con piena applicabilità prevista entro il 2 agosto 2026.

Tuttavia, alcune disposizioni, come i divieti, le disposizioni generali del Regolamento Europeo sull'IA, nonché gli obblighi per i fornitori di modelli di IA per le finalità generali sono già applicabili rispettivamente dal 2 febbraio 2025 e dal 2 agosto 2025.

REGOLAMENTO UE SULL'IA (AI Act)

L'AI Act classifica le applicazioni di IA in quattro livelli distinti:

- rischio inaccettabile
- alto rischio
- rischio limitato
- rischio minimo/nullo.

REGOLAMENTO UE SULL'IA (AI Act)

Il Regolamento UE sull'IA proibisce esplicitamente i sistemi di IA a "rischio inaccettabile"

- sistemi di inferenza delle emozioni che tentano di interpretare le emozioni degli studenti attraverso dati biometrici in contesti educativi (es. riconoscimento delle espressioni facciali, segnale vocale, stati fisiologici)
- sistemi che monitorano l'attenzione o l'interesse degli studenti.

REGOLAMENTO UE SULL'IA (AI Act)

- SISTEMI AD “ALTO RISCHIO”

Il settore dell'istruzione rientra nella categoria “Alto Rischio” per specifiche applicazioni di IA, a causa del loro impatto significativo sui diritti fondamentali degli studenti e sui loro percorsi educativi e professionali.

Esempio:

- sistemi che influenzano l'accesso alle opportunità educative (ad esempio sistemi di valutazione delle candidature, Sistemi di Orientamento e Reclutamento Personalizzato)
- sistemi che valutano i risultati dell'apprendimento (come software di correzione automatica, tutor intelligenti, piattaforme predittive)
- sistemi utilizzati per monitorare il comportamento o la disciplina scolastica.

Regolamento UE sull'IA (AI Act)

- SISTEMI A "rischi minimo o nullo"

Il rischio è considerato nullo quando l'AI svolge un ruolo di "suggeritore" o "facilitatore" e non di "decisore" o "profilatore critico".

Esempio:

- sistemi di puro supporto Amministrativo o Organizzativo (L'IA automatizza compiti di routine per il personale, senza prendere decisioni sullo studente)
- sistemi utilizzati come ausilio didattico, senza valutazioni (L'IA crea o adatta materiali, ma non valuta l'apprendimento in modo formale)
- sistemi con funzione Ricreativa o Ludica (L'IA è utilizzata per l'intrattenimento o per stimolare la partecipazione informale)
- sistemi di correzione di bassa importanza e con un controllo Umano (L'IA corregge solo aspetti oggettivi del lavoro, senza assegnare un voto finale determinante.)

REGOLAMENTO UE SULL'IA (AI Act)

- Da SISTEMI A “rischi minimo o nullo” a SISTEMI ad “alto rischio”

Un'applicazione apparentemente innocua può rientrare nella categoria ad “alto rischio” se:

- prevede la Profilazione: il sistema raggruppa gli studenti (es. "Studenti ad alto rendimento" vs. "Studenti a rischio di fallimento") e queste etichette influenzano le risorse o i percorsi futuri.
- il sistema viene utilizzato per assegnare un voto che contribuisce alla valutazione finale di uno studente o per determinare se uno studente viene ammesso o meno a un corso successivo;
- Utilizza la Biometria: anche se l'IA è solo un filtro anti-spam, se inizia a raccogliere e analizzare dati biometrici (es. analizzando il tono di voce dell'audio degli studenti) diventa immediatamente un sistema a rischio più elevato o addirittura vietato

RIEPILOGANDO:

Se l'applicazione nella scuola si limita a supportare il docente o ad assistere lo studente senza mai sostituire il giudizio umano o senza profilare gli utenti, il rischio è classificato come nullo o minimo

REGOLAMENTO UE SULL'IA (AI Act)

Classificazione dei Sistemi IA e Obblighi (AI Act)

<u>Categoria di Rischio</u>	<u>Definizione/Esempi in Ambito Educativo</u>	<u>Obblighi/Divieti Chiave</u>
Rischio Inaccettabile	Sistemi che minacciano chiaramente sicurezza, mezzi di sussistenza o diritti fondamentali.	<u>Proibiti:</u> Manipolazione dannosa, social scoring, sorveglianza biometrica (es. inferenza delle emozioni degli studenti, monitoraggio dell'attenzione in classe).
Alto Rischio	Applicazioni che potrebbero comportare gravi rischi per salute, sicurezza o diritti fondamentali.	<u>Obblighi Stringenti:</u> Sistemi per ammissione/selezione studenti, valutazione dei risultati di apprendimento (es. software di correzione automatica, tutor intelligenti, piattaforme predittive), monitoraggio del comportamento/disciplina scolastica. Richiedono rigorosi standard di sicurezza, affidabilità, accuratezza, supervisione umana e documentazione.

REGOLAMENTO UE SULL'IA (AI Act)

Classificazione dei Sistemi IA e Obblighi (AI Act)

<u>Categoria di Rischio</u>	<u>Definizione/Esempi in Ambito Educativo</u>	<u>Obblighi/Divieti Chiave</u>
Rischio Limitato	Sistemi con rischi limitati, soggetti a specifici obblighi di trasparenza	Obblighi di Trasparenza: Gli utenti devono essere consapevoli di interagire con un sistema IA (es. chatbot conversazionale sul sito web della scuola che risponde a domande complesse sul piano di studi, deepfake).
Rischio Minimo/Nulla	La maggior parte dei sistemi IA, che non presentano rischi significativi. La funzione del sistema è puramente ausiliaria, di supporto o ludica e non incide in modo significativo sulla valutazione o sui diritti fondamentali degli studenti	Nessun Obbligo Specifico: Possono essere immessi sul mercato senza requisiti normativi aggiuntivi. (es. es. Google Gemini o ChatGPT usati per generare bozze di testi o risposte a domande generiche).

REGOLAMENTO UE SULL'IA (AI Act)

MISURE DA ADOTTARE:

- avvio di un controllo di conformità dell'IA con i fornitori
 - definire le finalità del trattamento, la base giuridica
 - nominare il fornitore quale Responsabile Esterno del trattamento dei dati
 - verificare esistenza di un accordo sul trattamento dei dati- DPA (Data Processing Agreement)
- aggiornamento della documentazione interna (registro dei trattamenti, informative specifiche sulla privacy)
- formazione del personale sull'uso consapevole e trasparente dell'IA.

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE

(DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

L'IA può migliorare i processi **organizzativi, gestionali, formativi e di apprendimento**, contribuendo a qualificare le esperienze formative in modo inclusivo e accessibile.

Obiettivi del MIM:

- Promuovere un'IA **antropocentrica, sicura, affidabile, etica e responsabile;**
- Garantire la **conformità** alla normativa (AI Act e GDPR);
- Favorire la conoscenza delle opportunità e dei **rischi connessi all'utilizzo;**

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

RUOLO DELL'ISTITUZIONE SCOLASTICA:

L'Istituzione scolastica opera in qualità di «deployer», qualificato dall'art. 3, par. 1, n. 4, dell'AI Act, come «una persona fisica o giuridica, un'autorità pubblica, un'agenzia o un altro organismo che utilizza un sistema di IA sotto la propria autorità, tranne nel caso in cui il sistema di IA sia utilizzato nel corso di un'attività personale non professionale».

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

OBBLIGHI DEL DEPLOYER variano in base al livello di rischio dei sistemi di IA utilizzati:

- sistemi di IA ad alto rischio

I deployer sono tenuti a:

- utilizzare il sistema di IA in modo conforme, secondo le indicazioni del fornitore;
- garantire il monitoraggio del sistema di IA da parte di personale adeguatamente formato;
- eseguire una valutazione dell'impatto sui diritti fondamentali (c.d. "FRIA - Fundamental Rights Impact Assessment"), che l'uso del sistema di IA ad alto rischio può comportare (artt. 26 e 27, AI Act)

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

Sistemi di IA ad alto rischio

La **FRIA** (Fundamental Rights Impact Assessment) è lo strumento introdotto dall'AI ACT per valutare i rischi legati ai diritti fondamentali nell'uso dell'IA (art. 27 Reg. UE 2'24/1689-AI ACT). Essa è obbligatoria:

- Sistemi di AI ad Alto Rischio
- Soggetto responsabile: il Deployer che utilizza il sistema di AI

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE

(DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

DPIA

Valuta i rischi sui dati Personali e si applica quanto il trattamento è suscettibile di presentare un rischio elevato per i diritti e le libertà degli interessati (es. profilazione su larga scala, utilizzo di dati particolari o biometrici)

FRIA

Valuta i rischi sui Diritti fondamentali tutelati dall'UE, come il diritto alla non discriminazione, all'equità, alla dignità e all'accesso all'istruzione e si applica quanto si usa un sistema di AI ad Alto Rischio.

CONSIDERANDO 56 Reg. AI “ i sistemi di IA utilizzati nell'istruzione o nella formazione professionale, in particolare per determinare l'accesso o l'ammissione, per assegnare persone agli istituti o ai programmi di istruzione e formazione professionale a tutti i livelli, per valutare i risultati dell'apprendimento delle persone, per valutare il livello di istruzione adeguato per una persona e influenzare materialmente il livello di istruzione e formazione che le persone riceveranno o a cui potranno avere accesso o per monitorare e rilevare comportamenti vietati degli studenti durante le prove, dovrebbero essere classificati come sistemi di IA ad alto rischio, in quanto possono determinare il percorso d'istruzione e professionale della vita di una persona e quindi può incidere sulla sua capacità di garantire il proprio sostentamento

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

TUTELA DEI DIRITTI E DELLE LIBERTÀ FONDAMENTALI

L'utilizzo dell'Intelligenza Artificiale nelle Istituzioni scolastiche deve garantire:

- diritto alla protezione dei dati personali
- diritto alla riservatezza
- diritto alla non discriminazione
- diritto alla dignità della persona.

Pertanto i dati personali degli studenti e del personale scolastico devono essere trattati raccolti, conservati e trattati in modo trasparente, secondo i principi di minimizzazione e solo per finalità specifiche, esplicite e legittime legate alla funzione educativa e organizzativa delle scuole.

I sistemi di IA devono essere progettati secondo i principi di privacy by design e privacy by default, prevedendo configurazioni predefinite orientate alla massima tutela della privacy.

Devono inoltre essere adottate **misure** come la limitazione dei dati identificativi, l'anonimizzazione e l'uso di identificatori aggregati, per ridurre al minimo i rischi connessi al trattamento dei dati personali.

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

Nello specifico, un sistema di IA è considerato ad alto rischio se:

- presenta determinate caratteristiche/finalità, secondo quanto previsto dal Regolamento (i.e., art. 6, par. 1, AI Act e Allegato III all'AI Act). In particolare, nel settore dell'istruzione e della formazione professionale, il predetto

Allegato classifica ad alto rischio i sistemi utilizzati per:

- (i) determinare l'accesso, l'ammissione o l'assegnazione di persone fisiche agli istituti di istruzione e formazione professionale;

- (ii) valutare i risultati dell'apprendimento;

- (iii) valutare il livello di istruzione adeguato che una persona riceverà o a cui potrà accedere;

- (iv) monitorare e rilevare comportamenti vietati degli studenti durante le prove nel contesto o all'interno di istituti di istruzione e formazione professionale (cfr., anche Considerando 56 dell'AI Act);

- effettua la profilazione di persone fisiche;

- non sussiste almeno una delle condizioni di cui all'art. 6, par. 3, AI Act

LINEE GUIDA MIM PER L'INTRODUZIONE DELL'INTELLIGENZA ARTIFICIALE NELLE ISTITUZIONI SCOLASTICHE (DECRETO MINISTERIALE N. 166 DEL 9 AGOSTO 2025, AGGIORNATO IL 29.08.2025)

Sistemi di IA **NON** ad alto rischio che includono:

- sistemi a rischio limitato

L'AI Act impone precisi doveri di trasparenza, in modo tale che le persone fisiche interessate siano informate del fatto di stare interagendo con un sistema di IA

- sistemi a rischio minimo o nullo

Questi sistemi non hanno alcun impatto diretto sui diritti fondamentali o sulla sicurezza delle persone e offrono ampi margini di scelta e controllo agli utenti

EQUITÀ

Garanzia di pari accesso, inclusività, e mitigazione di eventuali **bias** o pregiudizi nei dati/modelli

CENTRALITÀ DELLA PERSONA

Approccio antropocentrico che garantisce il ruolo insostituibile dell'uomo nel governo dei sistemi

TUTELA DEI DIRITTI E DELLE LIBERTÀ FONDAMENTALI

Pieno rispetto del diritto alla protezione dei dati personali, alla riservatezza, e alla non discriminazione

I SEI PRINCIPI ETICI FONDANTI**SOSTENIBILITÀ**

Equilibrio tra sostenibilità sociale, economica e ambientale nel lungo termine

SICUREZZA DEI SISTEMI

Garanzia di elevati standard tecnici per proteggere dati e infrastrutture da accessi non autorizzati o attacchi

INNOVAZIONE ETICA E RESPONSABILE

Uso trasparente, consapevole che promuove l'apprendimento critico e creativo

I 4 PILASTRI DEL MODELLO DI INTRODUZIONE DELL'AI NELLE SCUOLE

Principi di Riferimento:

Principi generali per guidare l'adozione dell'IA nel rispetto dei valori

Requisiti di Base:

Requisiti in ambito etico, tecnico e normativo (GDPR) per assicurare un uso responsabile e sicuro

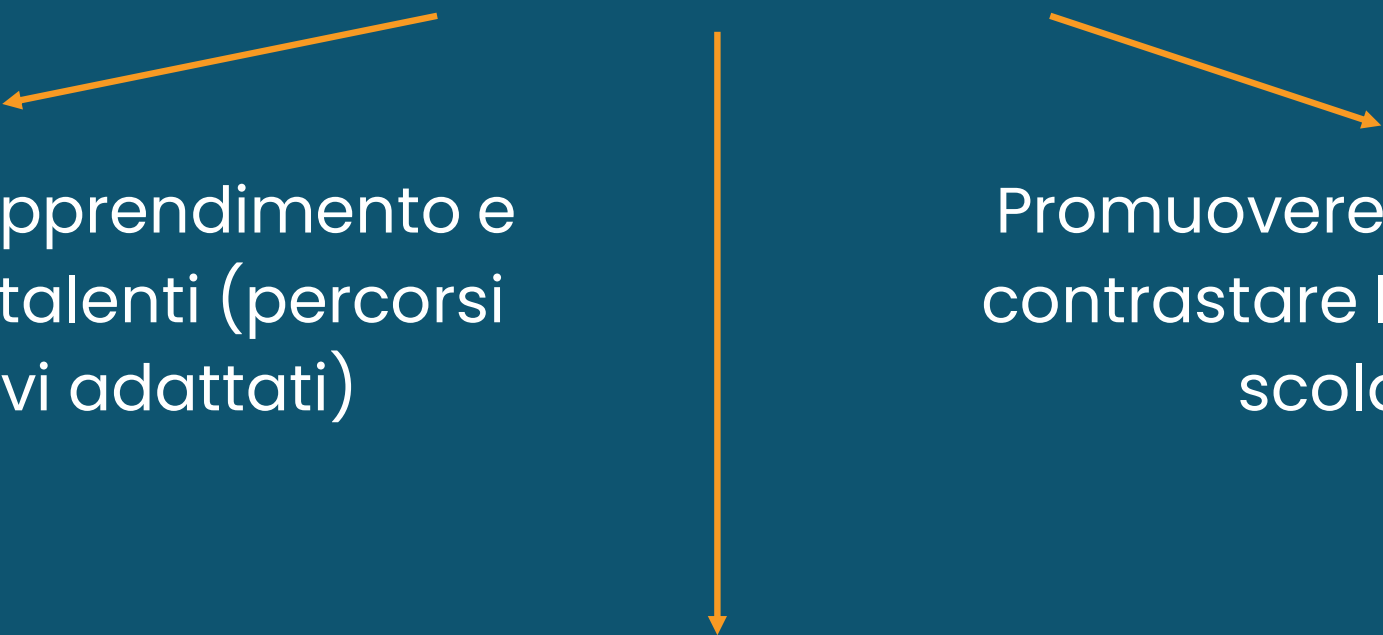
Framework di Implementazione:

Modello operativo e strumenti per supportare le Istituzioni scolastiche durante l'intero ciclo di vita dell'iniziativa

Comunicazione e Governance:

Adozione progressiva, consapevole e monitoraggio delle sperimentazioni (anche tramite la piattaforma Unica)

FINALITÀ D'IMPLEMENTAZIONE



```
graph TD; A[FINALITÀ D'IMPLEMENTAZIONE] --> B[Migliorare l'apprendimento e valorizzare i talenti (percorsi educativi adattati)]; A --> C[Promuovere l'inclusione e contrastare la dispersione scolastica]; A --> D[Semplificare e ottimizzare i processi amministrativi];
```

Migliorare l'apprendimento e valorizzare i talenti (percorsi educativi adattati)

Promuovere l'inclusione e contrastare la dispersione scolastica

Semplificare e ottimizzare i processi amministrativi

REQUISITI ETICI E RUOLI

- **Intervento e Sorveglianza Umana:** Il ruolo umano rimane centrale, in particolare per identificare anomalie, errori o discriminazioni (Responsabilità del Dirigente Scolastico);
- **Trasparenza e Spiegabilità:** I processi decisionali devono essere chiari, comprensibili e verificabili (audit) da parte degli utenti e delle autorità, che includono informazioni sul funzionamento e sulle procedure di monitoraggio e controllo adottate;
- **Criteri per evitare discriminazioni:** è necessario prestare attenzione alla qualità dei dati con cui l'IA viene addestrata ed esigere sistemi di controllo che permettano di individuare e correggere tempestivamente eventuali distorsioni

REQUISITI ETICI E RUOLI

- **Attribuzione di Ruoli e Responsabilità:**
 - a) **Dirigente Scolastico:** Responsabilità primaria nella *governance* e nel monitoraggio continuo. L'Istituzione agisce come Titolare del Trattamento;
 - b) **Coinvolgimento degli Utenti:** Le decisioni strategiche devono essere condivise con Studenti, Famiglie e Personale Scolastico tramite gli organi collegiali
 - c) **Accordi con i fornitori:** stabilire accordi chiari con i fornitori che definiscano il livello dei servizi di assistenza, manutenzione e le modalità di risoluzione di eventuali problemi. Nel caso in cui i fornitori assumano il ruolo di responsabili del trattamento, tali accordi dovranno includere anche gli elementi previsti dall'articolo 28 del Regolamento UE 2016/679 (di seguito, anche «GDPR»)

REQUISITI TECNICI

- **Requisiti tecnici:**

a) CERTIFICAZIONI E CONFORMITÀ DEI FORNITORI: La selezione del fornitore di sistemi IA deve basarsi su standard di sicurezza internazionali, come le certificazioni ISO/IEC 27001, e le qualificazioni particolarmente rilevanti nel contesto italiano, quali ad esempio la certificazione AgID per i servizi SaaS;

b) GESTIONE RESPONSABILE DEI DATI: verificare che i fornitori adottino pratiche trasparenti e conformi alla normativa vigente in materia di protezione dei dati personali, evitando utilizzi impropri dei dati per finalità diverse da quelle pattuite (tra le altre adesione al Data Privacy Framework)

REQUISITI TECNICI

- **Requisiti tecnici:**

- c) GESTIONE DEL DIRITTO DI NON PARTECIPAZIONE

Gli studenti e le loro famiglie devono avere la possibilità di decidere consapevolmente se i propri dati personali possano essere utilizzati per l'addestramento dei sistemi di IA

Deve essere garantito che tali scelte non comportino alcuna limitazione nell'accesso alle tecnologie didattiche stesse o agli strumenti di apprendimento basati sull'IA, come nel caso dei modelli linguistici di grandi dimensioni (LLM). In particolare, nel loro utilizzo è opportuno prevedere accorgimenti tecnici e organizzativi che evitino il trattamento di dati personali riconducibili agli studenti. L'inserimento di prompt deve avvenire preferibilmente senza trattamento di dati personali identificativi o riconducibili ad account individuali, in quanto può comportare rischi non compatibili con i principi di minimizzazione e limitazione della finalità.

Prevedere l'impiego di configurazioni che impediscano la conservazione dei prompt, la profilazione o il tracciamento degli studenti e assicurino un livello elevato di riservatezza.

REQUISITI NORMATIVI

RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

Il rispetto del diritto alla protezione dei dati personali risulta di fondamentale importanza nello sviluppo, nell'immissione sul mercato, nella messa in servizio e nell'uso di Sistemi di IA, che devono avvenire in conformità dei «principi chiave di protezione dei dati e della privacy osservati a livello internazionale» 5 come individuati dagli articoli 5 e 25 del GDPR.

La necessità di rispettare la normativa in materia di protezione dei dati personali nell'ambito dei Sistemi di IA è espressamente prevista all'interno delle seguenti fonti: tra cui l'AI ACT.

REQUISITI NORMATIVI

RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

“Il diritto alla vita privata e alla protezione dei dati personali deve essere garantito durante l'intero ciclo di vita del sistema di IA”:

- PRINCIPIO DI MINIMIZZAZIONE

- PROTEZIONE DEI DATI FIN DALLA PROGETTAZIONE E PER IMPOSTAZIONE PREDEFINITA (c.d. Privacy by Design e By Default)

Le misure adottate dai fornitori per garantire il rispetto di tali principi possono includere non solo l'anonimizzazione e la cifratura, ma anche l'uso di tecnologie che consentano di inserire algoritmi nei dati e di addestrare i sistemi di IA senza trasmissione tra le parti o copia degli stessi dati grezzi o strutturati, fatti salvi i requisiti in materia di governance dei dati di cui al presente regolamento» (Considerando 69)

REQUISITI NORMATIVI

RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

VERIFICA IN CAPO L'ISTITUZIONE SCOLASTICA:

Il trattamento dei dati effettuato mediante l'utilizzo dei Sistemi di IA è **NECESSARIO E PROPORZIONALE**?

Si rammenta che nel GDPR i minori sono indicati come persone fisiche «vulnerabili» (Considerando 75), pertanto meritevoli di «una specifica protezione relativamente ai loro dati personali, in quanto possono essere meno consapevoli dei rischi, delle conseguenze e delle misure di salvaguardia interessate nonché dei loro diritti in relazione al trattamento dei dati personali» (Considerando 38)

REQUISITI NORMATIVI

RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

VERIFICA IN CAPO L'ISTITUZIONE SCOLASTICA:

Se il trattamento dei dati effettuato mediante l'utilizzo dei Sistemi di IA riguarda i dati particolari di cui agli artt. 9 e 10 del GDPR?

Il trattamento dei dati è possibile solo nei casi strettamente indispensabili (i.e., al fine di supportare chi presenta difficoltà di apprendimento)

L'eventuale trattamento di tali categorie di dati potrà avvenire solamente previa adozione di specifiche misure tecnico – organizzative idonee a garantire un livello di sicurezza adeguato al rischio

REQUISITI NORMATIVI

RISPETTO DELLA NORMATIVA IN MATERIA DI PROTEZIONE DEI DATI PERSONALI

MISURE DI SICUREZZA PER I DATI PARTICOLARI:

- Cifratura (Crittografia): Adottare la cifratura end-to-end per i dati in transito e la cifratura at rest per i dati archiviati (sia nel database che nelle memorie di addestramento dell'AI)
- Pseudonimizzazione/Anonimizzazione: Utilizzare tecniche avanzate di pseudonimizzazione per sostituire gli identificativi diretti con pseudonimi. Se possibile e compatibile con gli obiettivi dell'AI, si deve preferire l'anonimizzazione completa per i dati non essenziali
- Controllo degli accessi più rigorosi (ad esempio Autenticazione a Multi-Fattore (MFA) per l'accesso ai sistemi AI e ai relativi dataset)
- Tracciabilità (Logging e Auditing): Assicurare che ogni accesso, modifica o decisione del sistema di AI (l'input di dati, l'output generato, e l'azione conseguente) sia registrato in modo immutabile (logging), permettendo la successiva verifica (audit). Questo è cruciale per la trasparenza richiesta dall'AI Act.
- Formazione specifica per il personale
- Supervisione umana (ad esempio una persona fisica sia in grado di intervenire, correggere o annullare le decisioni automatizzate che incidono sui diritti degli interessati)

PRINCIPALI ADEMPIMENTI PER L'ISTITUZIONE SCOLASTICA (DEPLOYER)

- individuazione di una specifica base giuridica
- esecuzione di una valutazione di impatto (DPIA)

Le Linee guida del MIM chiariscono inoltre che, ogni qual volta sussista un dubbio circa l'obbligatorietà o l'opportunità di effettuare la DPIA, sia sempre consigliabile, per il Titolare del Trattamento, procedere con lo svolgimento della stessa

Qualora le Istituzioni scolastiche intendano mettere in uso un Sistema di IA classificato come ad alto rischio ai sensi dell'articolo 6 dell'AI Act, sono tenute a integrare la DPIA con la valutazione d'impatto sui diritti fondamentali prevista dall'articolo 27 dell'AI Act (FRIA)

PRINCIPALI ADEMPIMENTI PER L'ISTITUZIONE SCOLASTICA (DEPLOYER)

In particolare, la FRIA, da integrare all'interno della DPIA, comprende, tra gli altri, i seguenti elementi: (i) la descrizione dei processi in cui il Sistema di IA ad alto rischio è utilizzato in linea con la sua finalità prevista; (ii) la descrizione del periodo di tempo entro il quale ciascun Sistema di IA ad alto rischio è destinato a essere utilizzato e con che frequenza; (iii) le categorie di persone fisiche e gruppi verosimilmente interessati dal suo uso nel contesto specifico; (iv) i rischi specifici di danno che possono incidere sulle categorie di persone fisiche o sui gruppi di persone individuati; (v) la descrizione dell'attuazione delle misure di sorveglianza umana, secondo le istruzioni per l'uso; (vi) le misure da adottare qualora tali rischi si concretizzino, comprese le disposizioni relative alla governance interna e ai meccanismi di reclamo

- rilascio agli interessati di un'idonea informativa sul trattamento dei dati personali eseguito nell'ambito deisistemi di IA

PRINCIPALI ADEMPIMENTI PER L'ISTITUZIONE SCOLASTICA (DEPLOYER)

- Nomina dei soggetti autorizzati al trattamento dei dati personali: nell'ambito dei progetti che saranno attivati in materia di IA, l'Istituzione scolastica, in qualità di Titolare del Trattamento, può individuare e autorizzare uno o più soggetti, particolarmente qualificati, allo svolgimento delle attività legate al trattamento, fornendo agli stessi specifiche istruzioni
- Nomina dei responsabili del trattamento dei dati personali
- Adozione di misure tecnico-organizzative
- Tenuta del registro delle attività del trattamento
- Notifica delle violazioni dei dati personali al Garante e comunicazione agli interessati

PIATTAFORMA UNICA CHECK-LIST

Nella sezione “Sperimentazioni AI” i dirigenti scolastici e il personale amministrativo possono registrare nuovi progetti sull’Intelligenza Artificiale compilando una scheda dedicata, e verificando la conformità normativa grazie ad una check list.

La checklist si compone di 34 elementi suddivisi per aree tematiche (principi generali, diritti degli interessati, valutazione d’impatto, ruoli e responsabilità, sicurezza e accountability)

SCOPO: autovalutazione per le scuole che intendono introdurre l’IA in classe.

PIATTAFORMA UNICA CHECK-LIST

PRINCIPI GENERALI DEL TRATTAMENTO (art. 5 GDPR)

- Liceità del trattamento dei dati personali.
- Correttezza del trattamento.
- Trasparenza verso gli interessati.
- Limitazione delle finalità.
- Minimizzazione dei dati.
- Esattezza e aggiornamento dei dati.
- Limitazione della conservazione.
- Integrità e riservatezza dei dati

GARANZIE PER GLI INTERESSATI E TRASPARENZA

- Comprensibilità e conoscibilità delle informazioni (art. 12 GDPR)
- Non esclusività delle decisioni automatizzate (art. 22 GDPR).
- Assenza di discriminazioni algoritmiche o bias nei sistemi IA.
- Base giuridica del trattamento chiaramente definita.
- Presenza di un'informativa agli interessati (artt. 13 e 14 GDPR).
- Chiarezza dei diritti degli interessati (accesso, rettifica, cancellazione, opposizione).
- Procedure di esercizio dei diritti e moduli dedicati disponibili.

PIATTAFORMA UNICA CHECK-LIST

VALUTAZIONE D'IMPATTO E GESTIONE DEL RISCHIO

- Valutazione d'impatto sulla protezione dei dati (DPIA) redatta e aggiornata.
- Valutazione d'impatto sui diritti fondamentali (FRIA) per sistemi ad alto rischio.
- Individuazione delle categorie di dati trattati.
- Descrizione chiara delle finalità del trattamento.
- Identificazione del titolare, del RPD e dei responsabili esterni.
- Analisi della proporzionalità e necessità dei trattamenti.
- Individuazione e classificazione dei rischi connessi all'uso dei sistemi IA.

RUOLI E RESPONSABILITÀ

- Nomina formale dei soggetti autorizzati al trattamento (personale interno).
- Nomina dei responsabili esterni ai sensi dell'art. 28 GDPR.
- Contratti o atti giuridici con i fornitori IA contenenti garanzie adeguate.
- Definizione delle istruzioni operative interne (policy e regolamento IA).
- Tenuta del Registro delle attività di trattamento.

PIATTAFORMA UNICA CHECK-LIST

MISURE DI SICUREZZA TECNICHE E ORGANIZZATIVE

- Adozione di misure di sicurezza informatica (crittografia, controllo accessi, log).
- Applicazione del principio di data protection by design e by default.
- Formazione e sensibilizzazione del personale sul trattamento dati e IA.
- Procedure di gestione e notifica di violazioni dei dati personali (data breach).
- Sistemi di monitoraggio, revisione e aggiornamento periodico delle misure.

F. DIRITTI, COMUNICAZIONE E DOCUMENTAZIONE

- Comunicazione agli interessati in caso di data breach (art. 34 GDPR).
- Conservazione della documentazione relativa a tutte le misure adottate (accountability)

CRITICITÀ RISCONTRATE NEI SISTEMI AI

Criticità riscontrate nell'utilizzo delle versioni non Enterprise o gratuite:

- a) i dati degli studenti/ docenti vengono usati per addestrare l'AI e, dunque, per le finalità commerciali e di sviluppo dell'applicazione. Questo implica che il fornitore/azienda agisce come Titolare del trattamento per i dati che usa per addestrare l'AI in quanto i dati vengono usati per fini propri, con conseguente perdita di controllo sui dati personali degli studenti da parte della scuola;
- b) il fornitore non assume il ruolo di Responsabile esterno del trattamento dei dati;
- b) assenza di un accordo sul trattamento dei dati (DPA) che contenga, tra le altre, l'atto di nomina del fornitore come responsabile esterno del trattamento dei dati personali, clausole essenziali nelle quali il fornitore si impegna a non utilizzare i dati degli utenti per addestrare i modelli di intelligenza artificiale.

CRITICITÀ RISCONTRATE NEI SISTEMI AI

Se il docente utilizza l'applicazione AI solo per generare materiali didattici, piani di lezione o contenuti testuali che non contengono alcun dato personale degli studenti, la responsabilità ricade sul docente come utente finale. In tal caso l'uso non coinvolge i dati degli studenti. Viceversa, se il docente utilizza l'applicazione per:

- a) caricare o inserire dati identificativi degli studenti (nomi, voti, performance individuali) per ottenere feedback o analisi (ad esempio, usa Claude per correggere un tema e inserisce il nome dello studente);
- b) chiedere agli studenti di usare l'applicazione (anche se la versione è gratuita) per un'attività curricolare, costringendoli a creare un account o inserire i loro input:

l'uso dell'applicazione non è conforme al GDPR. Anche se il docente agisce autonomamente, sta utilizzando dati personali degli studenti (dati della scuola) e li sta trasferendo a un fornitore terzo (Titolare Autonomo), senza che la scuola abbia stipulato il necessario Accordo sul Trattamento dei Dati (DPA).

CONFORMITÀ AL GDPR

- **Utilizzare una Versione Business/Enterprise/Edu:** È essenziale usare una versione che non utilizzi i dati degli studenti per l'addestramento dei modelli di OpenAI.
- **Stipulare il DPA:** Formalizzare il **Data Processing Addendum** con il fornitore del servizio di AI per la nomina a Responsabile Esterno ogni qualvolta l'applicazione preveda l'inserimento dei dati personali degli studenti.
- **Eseguire una DPIA:** La scuola deve condurre una **Valutazione d'Impatto sulla Protezione dei Dati (DPIA)** a causa dell'uso di una tecnologia innovativa e potenzialmente ad alto rischio (IA generativa).
- **Assicurare la Sorveglianza Umana:** Garantire che l'uso del sistema di AI sia sempre supervisionato dall'insegnante e che l'IA non sia mai utilizzata per prendere decisioni in autonomia (es. valutazioni finali) in conformità con i principi dell'AI Act e del GDPR.
- **Informare gli Interessati:** Fornire un'**Informativa Privacy** chiara ai genitori/studenti sulla modalità d'uso e sulla base giuridica (basata in tal caso sull'esecuzione di un compito di interesse pubblico).

ESEMPI DI ALCUNE APP VERIFICATE

CHAT GPT
GEMINI FOR EDUCATION
CLAUDE (Anthropic)
COPILOT
NOTEBOOK LM
PERPLEXITY
GAMMA
MENTIMETER
TEACHABLE MACHINE GOOGLE
MAGIC SCHOOL
CANVA FOR EDUCATION
NAPKIN
ALGOR
DEBATAI
ELEVENLABS
PANQUIZ (Azienda Italiana)
MOODLE (software open source)

EDPUZZLE
SUNO
HABLA CON LA HISTORIA
TWEE
GENIALLY
AI DOCENTI
GRAMMARLY
DUOLINGO
SLIDESAI.IO
ALMANACK.AI
EDUAIDE.AI
NOTEGPT
WONDERCRAFT.AI
MIZOU
ANK

PER INFORMAZIONI E CHIARIMENTI

info@eduservice.it

avv.alessandralezzi@eduservice.it