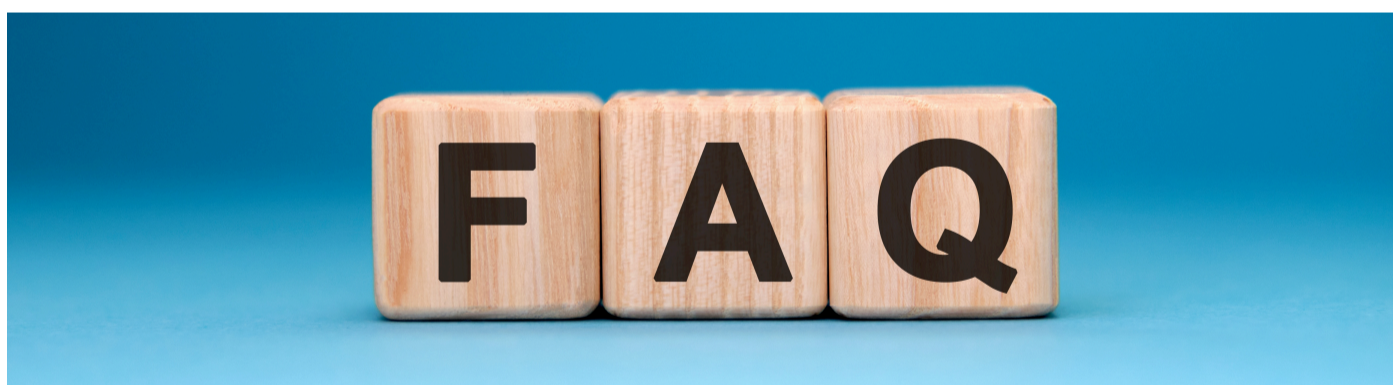




Esami e corsi a distanza

[Home](#) / [Temi](#) / [Istruzione e formazione](#) / [Esami e corsi a distanza](#)



FAQ: Sistemi di supervisione per la regolarità di prove d'esame e corsi a distanza

Le università pubbliche e private e gli enti di formazione possono svolgere prove d'esame e corsi a distanza? Sono ammessi sistemi di monitoraggio dei comportamenti dei partecipanti? Possono essere raccolte le immagini di studenti e lavoratori che seguono le attività di formazione? A queste e ad altre domande rispondono le FAQ pubblicate dal Garante privacy. L'obiettivo è quello di chiarire le modalità di utilizzo dei sistemi di supervisione per la regolarità delle prove d'esame e dei corsi a distanza.

1. Possono università pubbliche e private ed altri enti che perseguono finalità di interesse pubblico svolgere prove d'esame e corsi a distanza?

Si, i trattamenti di dati di persone fisiche (studenti, partecipanti, candidati, ecc.), finalizzati al rilascio di titoli di studio aventi valore legale, nonché di titoli abilitanti o attestati la frequenza a lezioni, corsi e attività di formazione in genere, anche nel quadro di attività soggette alla vigilanza di soggetti pubblici (in particolare, il Ministero dell'istruzione e del merito, il Ministero dell'Università e della Ricerca o altri enti che hanno competenza in materia

di formazione e istruzione, anche a livello locale), trovano la loro base giuridica - indipendentemente dalla natura pubblica o privata del titolare del trattamento - nella necessità di eseguire obblighi di legge o svolgere i propri compiti di interesse pubblico (v. artt. 6, par. 1, lett. c) ed e), e art. 9, par. 2, lett. g), del Regolamento (UE) 2016/679 - di seguito, "Regolamento" - nonché artt. 2-ter e 2-sexies, comma 2, lett. bb) e g), del d.lgs. 30 giugno 2003, n. 196, Codice in materia di protezione dei dati personali - di seguito, "Codice"). Tali trattamenti non possono, invece, trovare fondamento in altre basi giuridiche quali il consenso, il contratto o il legittimo interesse (cfr. art. 6, par. 1, lett. a), b) e f), del Regolamento).

Lo svolgimento di prove d'esame e corsi, sia pure in ambiente virtuale e a distanza, mediante strumenti telematici e piattaforme digitali, rientra tra le attività istituzionalmente assegnate a università, enti di alta formazione e altri enti abilitati, i quali sono, pertanto, legittimati a trattare i dati personali necessari all'esecuzione dei propri compiti di interesse pubblico.

Ciò deve, comunque, avvenire nei limiti del quadro normativo di settore, nella misura in cui i trattamenti di dati personali siano strettamente necessari ai fini del regolare svolgimento della prova, impiegando, ad esempio, servizi di videoconferenza o piattaforme che non consentano la raccolta di dati non pertinenti (es. la posizione geografica o i dati biometrici dei candidati), non effettuino ulteriori elaborazioni e comunque senza utilizzare funzionalità non necessarie che aggravino, in maniera ingiustificata, i rischi per i diritti e le libertà degli interessati rispetto al tradizionale svolgimento delle prove in presenza. Gli strumenti informatici utilizzati devono essere, pertanto, configurati in modo da non porre in essere trattamenti non necessari, minimizzando, altresì, i dati personali da trattare e i tempi dell'eventuale loro conservazione alla luce della predetta finalità d'interesse pubblico perseguita (ad esempio, impostazioni della videocamera, limitazione dell'inquadratura, risoluzione, eventuale disattivazione della registrazione ove non necessaria).

2. È possibile trattare dati personali mediante sistemi di supervisione (c.d. "proctoring") nell'ambito dello svolgimento di prove e corsi a distanza?

Sì, i sistemi digitali di supervisione delle prove d'esame e dei corsi a distanza consistono in specifici programmi informatici funzionali alla verifica della regolare partecipazione e dello svolgimento degli stessi; in taluni casi, tali programmi possono, altresì, consentire l'identificazione di ciascuna persona fisica che partecipa al corso o sostiene la prova (c.d. "proctoring").

Il sempre più frequente ricorso a tali sistemi può presentare particolari rischi per i diritti e le libertà degli interessati, in quanto alcune soluzioni tecnologiche disponibili sul mercato prevedono, ad esempio, il trattamento di categorie particolari di dati, come quelli biometrici, il ricorso alla profilazione, l'adozione di decisioni automatizzate nei confronti degli interessati, il trasferimento internazionale dei dati verso Paesi terzi, o, comunque, trattamenti diversi e ulteriori da quelli strettamente necessari per il mero svolgimento a distanza delle prove d'esame e dei corsi.

In assenza di un adeguato quadro normativo che individui, anzitutto, i contesti nei quali il ricorso a tali sistemi sia effettivamente necessario per il perseguimento delle finalità di interesse pubblico connesse al regolare svolgimento delle prove d'esame e dei corsi, e che definisca le necessarie garanzie per i diritti e le libertà degli interessati a fronte dei rischi che incombono sugli stessi, i titolari del trattamento devono valutare, anche avvalendosi del supporto del Responsabile della protezione dei dati (RPD), ove designato, le specifiche funzionalità e caratteristiche del sistema che intendono utilizzare, nel rispetto dei principi generali di protezione dei dati. Inoltre, con specifico riguardo ai principi di responsabilizzazione e di protezione dei dati fin dalla progettazione e per impostazione predefinita, i titolari, già in sede di selezione del sistema di supervisione da impiegare, devono tenere conto delle specifiche caratteristiche, anche tecniche, dello stesso, prediligendo quei sistemi che, sia nella fase di progettazione che di sviluppo successivo, abbiano caratteristiche e funzionalità tali da consentire ai titolari di adempiere agli obblighi di protezione dei dati (cfr. cons. 78 e artt. 5 e 25 del Regolamento).

Il titolare deve comunque adottare le misure tecniche e organizzative che garantiscano la conformità dei trattamenti alla disciplina di protezione dei dati, anche quando siano utilizzati sistemi offerti da terzi. In tali casi, ciascun fornitore del servizio deve essere qualificato quale responsabile del trattamento ai sensi dell'art. 28 del Regolamento, ove ne ricorrano i presupposti. In tale contesto, occorre impartire al responsabile le necessarie istruzioni, assicurando che siano, ad esempio, disattivate le funzioni che possono dare luogo a trattamenti privi di

base giuridica o non compatibili con le finalità del trattamento, privilegiando il ricorso a soluzioni che si limitino a inibire specifiche funzionalità dei dispositivi in uso agli interessati nel corso dello svolgimento della prova d'esame o nel contesto della partecipazione al corso (ad esempio, impedendo l'apertura di finestre diverse da quella su cui si svolge la prova d'esame o il corso oppure disabilitando specifiche funzionalità del sistema operativo, come l'operazione di copia e incolla), senza tenere traccia delle operazioni effettuate dagli interessati (ad esempio, delle attività sul web, delle applicazioni utilizzate, dei tasti digitati sulla tastiera e dei movimenti o click del mouse, ecc.).

A seconda dello specifico contesto di riferimento (numero dei partecipanti al corso o iscritti alla sessione d'esame; tipologia di corso o di prova; alternative disponibili; ecc.), il titolare potrà, altresì, valutare la necessità di effettuare una registrazione audio-video dell'esame (anche riprendendo il volto della persona che partecipa al corso o sostiene la prova, senza estrazione di dati biometrici), individuando un congruo termine di conservazione delle registrazioni (art. 5, par. 1, lett. e), del Regolamento), tenuto conto, in particolare, dei termini previsti dalla legge per impugnare l'esito della prova o il mancato riconoscimento della frequenza al corso (reclamo alla commissione esaminatrice oppure ricorso al TAR), nonché prevedendo adeguate misure di sicurezza per le medesime registrazioni (es. limitazioni di accesso).

Qualora il sistema comporti un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare è tenuto a svolgere una valutazione d'impatto sulla protezione dei dati (DPIA) ai sensi dell'art. 35 del Regolamento (cfr. [FAQ n. 6](#)).

In ogni caso, i sistemi non devono comportare un'eccessiva ingerenza nella sfera dell'interessato e un monitoraggio invasivo dell'attività dello stesso, configurando un trattamento sproporzionato rispetto alle effettive finalità d'interesse pubblico perseguite (cfr. Memoria del Presidente del Garante del 27 aprile 2021 presso le Commissioni riunite 7a e 12a del Senato in tema di "Impatto della didattica digitale integrata (DDI) sui processi di apprendimento e sul benessere psicofisico degli studenti", doc. web n. [9581498](#), spec. par. 3).

3. Possono essere trattati dati biometrici di studenti e partecipanti ai corsi e alle prove d'esame mediante tali sistemi?

No, considerato che, in base al quadro normativo in materia di protezione dei dati personali, il trattamento dei dati biometrici, di regola vietato, in quanto tali dati rientrano tra le categorie particolari di dati di cui all'art. 9, par. 1, del Regolamento, è ammesso, in tale contesto, solo se espressamente previsto da un'idonea base giuridica che individui, tra l'altro, il motivo di interesse pubblico rilevante che giustifica il trattamento, nonché preveda specifiche garanzie a tutela degli interessati (cfr. art. 9 del Regolamento e 2-sexies, commi 1 e 2, lett. bb) e g) del Codice).

Per tali ragioni, in assenza di una specifica base giuridica, idonea per rango e qualità (v. artt. 6, parr. 2 e 3, del Regolamento, nonché 2-ter e 2-sexies del Codice), non è consentito l'utilizzo di sistemi di supervisione che comportino il trattamento di dati biometrici degli interessati (ad esempio, mediante la tecnologia di riconoscimento facciale) per l'identificazione degli stessi oppure per la rilevazione di eventi anomali (es. sostituzione di persona) nel corso delle lezioni o della prova (cfr. provv.ti 29 gennaio 2026, n. 35, doc. web n. [10221611](#), citato anche in Newsletter 20 febbraio 2026, doc. web n. [10222071](#), e 16 settembre 2021, n. 317, doc. web n. [9703988](#), confermato da Cass. civ., Sez. I, n. sent. n. 12967 del 13 maggio 2024 e, a seguito del rinvio, da Tribunale di Milano, sent. n. 8872, del 20 gennaio 2026).

4. Sono ammessi sistemi che comportano trattamenti automatizzati di dati personali per analizzare e prevedere il comportamento degli interessati?

No, in quanto il trattamento automatizzato di dati personali per valutare e analizzare aspetti riguardanti il comportamento di una persona fisica (cfr. art. 4, n. 4, del Regolamento in materia di profilazione) è ammesso, in tale contesto, solo se il trattamento è necessario per l'esecuzione di un compito di interesse pubblico e previsto da una base giuridica idonea per rango e qualità. Ciò anche in considerazione dei rischi per gli interessati, i quali, in conseguenza di tali trattamenti, possono subire conseguenze pregiudizievoli, come il mancato riconoscimento della frequenza al corso o l'annullamento di una prova d'esame.

Per tali ragioni, anche nel caso in cui sia prevista la successiva valutazione in concreto dell'effettiva presenza ai corsi e della condotta del partecipante da parte del docente o della commissione esaminatrice, non è consentito, in assenza di idonea base giuridica, l'utilizzo di sistemi di supervisione che comportano la raccolta e l'elaborazione di

dati relativi al comportamento dello studente durante la prova d'esame (ad esempio, movimenti del corpo, frequenza dei movimenti o click del mouse, operazioni compiute sulla tastiera, tentativi di accesso ad altre applicazioni, attività su Internet, ecc.), mediante algoritmi idonei a generare informazioni nuove e ulteriori rispetto a quelle direttamente fornite dall'interessato, al fine di elaborare indici di rischio o segnali di allerta relativi a possibili comportamenti fraudolenti.

Resta fermo che i processi decisionali interamente automatizzati devono rispettare le condizioni previste dall'art. 22 del Regolamento, nonché, ove ne ricorrano i presupposti, in requisiti previsti dalla disciplina europea e nazionale in materia di intelligenza artificiale (Regolamento (UE) 2024/1689 e l. 23 settembre 2025, n. 132).

5. È possibile fare ricorso a fornitori di sistemi di supervisione che sono stabiliti al di fuori dell'Unione europea?

Sì, ma solo a condizione che ricorrano le condizioni previste dalla normativa in materia di protezione dei dati (v. artt. 44-49 del Regolamento; cfr. la sezione "Trasferimento di dati personali all'estero" sul sito web del Garante; v. anche le indicazioni fornite dal Comitato europeo per la protezione dei dati, tra cui le "Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE" del 18 giugno 2021).

6. Il titolare del trattamento deve svolgere una valutazione di impatto sulla protezione dei dati per lo svolgimento di corsi o prove d'esame a distanza o per l'impiego di sistemi di supervisione?

La valutazione di impatto sulla protezione dei dati (cfr. art. 35 del Regolamento) non è necessaria nei casi in cui il titolare si limiti a trattare i dati personali che sono strettamente necessari ai fini dello svolgimento di corsi o prove d'esame a distanza, in particolare, mediante servizi online di videoconferenza o di piattaforme che non consentono il monitoraggio automatizzato degli interessati, o comunque non faccia ricorso a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano il trattamento di dati biometrici).

Diversamente, in caso di impiego di sistemi di supervisione della partecipazione ai corsi e dello svolgimento delle prove d'esame a distanza ("proctoring"), il titolare, prima di iniziare il trattamento, deve svolgere una valutazione di impatto sulla protezione dei dati, considerato l'utilizzo di nuove tecnologie e il monitoraggio sistematico che l'impiego di tali sistemi può comportare, nonché la possibile ricorrenza delle condizioni individuate dall'art. 35, par. 3, del Regolamento (in particolare il monitoraggio sistematico su larga scala di una zona accessibile al pubblico o la valutazione sistematica e globale di aspetti personali).

Qualora dalla valutazione emerga un rischio elevato residuo non mitigabile con misure adeguate, il titolare è, inoltre, tenuto a consultare preventivamente l'Autorità di controllo ai sensi dell'art. 36 del Regolamento.

7. È necessario fornire un'informativa specifica agli studenti e ai partecipanti ai corsi a distanza?

Sì. Il titolare del trattamento deve fornire agli interessati un'informativa chiara e trasparente ai sensi degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento, che indichi, tra l'altro, le finalità del trattamento, la base giuridica, le modalità di svolgimento delle prove o dei corsi a distanza, l'eventuale utilizzo di sistemi di supervisione, i tempi di conservazione dei dati, i soggetti destinatari e l'eventuale trasferimento dei dati verso Paesi terzi.

Qualora siano impiegati sistemi di proctoring o strumenti che comportino forme di monitoraggio, l'informativa deve descrivere in modo specifico le funzionalità utilizzate e i dati effettivamente trattati, nel rispetto del principio di correttezza e trasparenza.

8. Devono essere adottate specifiche misure di sicurezza per lo svolgimento di esami a distanza?

Sì. Ai sensi dell'art. 32 del Regolamento, il titolare deve adottare misure tecniche e organizzative adeguate al rischio, quali, ad esempio: adottare procedure di autenticazione robusta per l'accesso alle piattaforme digitali; assicurare la tracciabilità degli accessi e delle operazioni compiute sui dati, nei limiti di quanto necessario e proporzionato; definire policy di conservazione e cancellazione coerenti con il principio di limitazione della conservazione (art. 5, par. 1, lett. e), del Regolamento); verificare che i fornitori di servizi digitali impiegati offrano

garanzie adeguate in termini di sicurezza, anche mediante specifiche clausole contrattuali ai sensi dell'art. 28 del Regolamento; prevedere programmi di formazione e istruzione del personale coinvolto nelle attività didattiche e valutative a distanza.

Faq

1 Possono università pubbliche e private ed altri enti che perseguono finalità di interesse pubblico svolgere prove d'esame e corsi a distanza?
2 È possibile trattare dati personali mediante sistemi di supervisione (c.d. "proctoring") nell'ambito dello svolgimento di prove e corsi a distanza?
3 Possono essere trattati dati biometrici di studenti e partecipanti ai corsi e alle prove d'esame mediante tali sistemi?
4 Sono ammessi sistemi che comportano trattamenti automatizzati di dati personali per analizzare e prevedere il comportamento degli interessati?
5 È possibile fare ricorso a fornitori di sistemi di supervisione che sono stabiliti al di fuori dell'Unione europea?
6 Il titolare del trattamento deve svolgere una valutazione di impatto sulla protezione dei dati per lo svolgimento di corsi o prove d'esame a distanza o per l'impiego di sistemi di supervisione?
7 È necessario fornire un'informativa specifica agli studenti e ai partecipanti ai corsi a distanza?
8 Devono essere adottate specifiche misure di sicurezza per lo svolgimento di esami a distanza?

Temi

[Banche, credito, finanza](#)

[Biometria](#)

[Creative Commons](#)

[Cyberbullismo](#)

[Cybersecurity](#)

[Fisco](#)

[Giornalismo](#)

[Informazioni commerciali](#)

[Iniziative formative](#)

[AI - Intelligenza artificiale](#)

[Internet e nuove tecnologie](#)

[Istruzione e formazione](#)

[Istruzione e formazione](#)

[Scuola](#)

[Esami e corsi a distanza](#)

[Cyberbullismo](#)

[Lavoro](#)

[Marketing e comunicazioni
indesiderate](#)

[Minori](#)

[Pubblica amministrazione e
trasparenza](#)

[Revenge Porn](#)

[Sanità e Ricerca scientifica](#)

[Trasferimento di dati personali all'estero](#)

[Trasporti](#)

[Videosorveglianza](#)

[GDPR - Regolamento
2016/679](#)

[Codice Privacy](#)

[Dalla A-Z](#)

[Posta elettronica](#)



GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

SEDE

Piazza Venezia 11
00187 - Roma

CENTRALINO TELEFONICO

+39 06.696771

> [URP](#)

> [FAQ](#)

> [RSS](#)

EMAIL

protocollo@gdpd.it

PEC

protocollo@pec.gdpd.it

> [Informativa protezione dati](#)

> [Dichiarazione di accessibilità](#)

> [Regole del sito](#)

> [Mappa del sito](#)

> [Link utili](#)

Seguici su



[Iscriviti alla Newsletter](#)