



# Ministero dell'istruzione e del merito

*Dipartimento per le risorse, l'organizzazione e l'innovazione digitale*

*Dipartimento per il sistema educativo di istruzione e formazione*

## **ALLEGATO 1**

### **VADEMECUM REGISTRO ELETTRONICO**

#### **1) Procedura di identificazione e autenticazione**

In coerenza con quanto previsto dall'art. 24, comma 4, del D.L. n. 76/2020 e dall'art. 64 del CAD, l'accesso al Registro deve avvenire **esclusivamente** mediante l'utilizzo di identità digitali (i.e., SPID, CIE, eIDAS).

Tali modalità di accesso, infatti, consentono di **garantire un adeguato livello di sicurezza**, impedendo o limitando l'accesso al Registro medesimo a soggetti non autorizzati. A tal fine è importante che, progressivamente, l'identità digitale diventi la preponderante modalità di accesso al registro.

Si ricorda inoltre che, al fine di semplificare gli adempimenti tecnico-amministrativi, il Ministero ha messo a disposizione delle Istituzioni Scolastiche e dei Fornitori che implementano pacchetti *software* una piattaforma di autenticazione c.d. «Gateway delle identità» o «eID Gateway», che agevola l'integrazione con i sistemi «Entra con SPID», «Entra con CIE» e «Login with eIDAS», facilitando l'accesso alle applicazioni con cui le Istituzioni medesime erogano servizi a studentesse e studenti, genitori, docenti e personale scolastico.

Ai fini di cui sopra, il suddetto «Gateway delle identità» supporta anche l'utilizzo dello SPID Minori, consentendo agli alunni e agli studenti minorenni di poter utilizzare i servizi sia tramite SPID che CIE.

#### **2) Interoperabilità e integrazione con gli ulteriori servizi resi disponibili dal Ministero**

Ai sensi di quanto previsto dagli artt. 12 e 64-*bis* del CAD, il Registro deve essere interoperabile con le applicazioni digitali del Ministero, al fine di assicurare la qualità, la continuità e la condivisione dei servizi offerti dal Ministero medesimo nei confronti di studentesse e studenti, genitori, dirigenti scolastici e personale scolastico.

In particolare, il Registro deve consentire l'interoperabilità con il Sistema Informativo dell'Istruzione (SIDI), utilizzato per monitorare, gestire e fornire servizi legati al mondo della scuola e con le principali applicazioni in uso quali ad esempio, l'Anagrafe Nazionale degli Studenti (ANS), la Piattaforma Unica, il servizio Pago In Rete.

#### **3) Accessibilità**

Il Registro deve garantire il rispetto delle previsioni in materia di accessibilità dei siti web e delle applicazioni mobili per le persone con disabilità, al fine di erogare Servizi fruibili, senza discriminazioni, nei confronti dell'intera platea di utenti (i.e., Legge del 9 gennaio 2004, n. 4, recante «Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici»; D.Lgs. n. 106/2018, recante «Attuazione della direttiva (UE) 2016/2102 relativa all'accessibilità dei siti web e delle applicazioni mobili degli enti pubblici»; Linee Guida sull'accessibilità degli strumenti informatici, adottate dall'Agenzia per l'Italia Digitale, da ultimo aggiornate il 29 maggio 2023, che definiscono i requisiti tecnici per l'accessibilità degli strumenti informatici, ivi inclusi i siti web e le applicazioni mobili).

#### **4) Data Protection**

Le Istituzioni Scolastiche, in relazione ai trattamenti effettuati per il tramite del Registro, ricoprono la funzione di Titolari del trattamento dei dati personali, in quanto, ai sensi dell'art. 4, par. 1, n. 7, del GDPR, determinano le



# Ministero dell'istruzione e del merito

*Dipartimento per le risorse, l'organizzazione e l'innovazione digitale*

*Dipartimento per il sistema educativo di istruzione e formazione*

finalità e i mezzi del trattamento di dati personali. Per tale motivo, devono garantire che i Servizi affidati siano rispettosi dei principi in materia di protezione dei dati personali come riportati all'interno dell'art. 5 del GDPR ossia: (i) liceità, correttezza e trasparenza nel trattamento dei dati personali dell'interessato, (ii) limitazione della finalità; (iii) minimizzazione dei dati, (iv) esattezza dei dati, (v) limitazione della conservazione, (vi) integrità e riservatezza nel trattamento dei dati e (vii) responsabilizzazione.

Tra i principali adempimenti che le Istituzioni Scolastiche, nell'ambito della propria autonomia didattica e organizzativa, sono tenute ad eseguire in qualità di Titolari, si segnalano i seguenti:

- (i) esecuzione di una valutazione di impatto sul trattamento dei dati personali (DPIA), al fine di individuare i rischi connessi al trattamento eseguito (artt. 35 e ss. del GDPR);
- (ii) rilascio agli interessati di un'ideona informativa sul trattamento dei dati personali, ai sensi degli artt. 13 e 14 del GDPR;
- (iii) nomina dei soggetti autorizzati al trattamento dei dati personali (art. 29 del GDPR e art. 2-*quaterdecies* del D.Lgs. n. 196/2003).

Per adempiere a tali attività, le Istituzioni Scolastiche possono opportunamente coinvolgere anche i rispettivi «*Data Protection Officer*».

Le Istituzioni Scolastiche nominano, inoltre, all'interno di uno specifico contratto o altro atto giuridico, i Fornitori quali Responsabili del trattamento dei dati, che ai sensi dell'art. 28 del GDPR, a titolo esemplificativo, provvedono a:

- (a) trattare i dati personali per le sole finalità specificate e nei limiti dell'esecuzione delle prestazioni contrattuali;
- (b) garantire la riservatezza dei dati personali trattati nell'ambito del contratto e verificare che le persone autorizzate a trattare i dati personali in virtù del contratto: (i) si impegnino a rispettare la riservatezza o siano sottoposti a un obbligo legale appropriato di segretezza, (ii) ricevano la formazione necessaria in materia di protezione dei dati personali e (iii) trattino i dati personali osservando le istruzioni impartite dal Titolare;
- (c) informare il Titolare tempestivamente e, in ogni caso senza ingiustificato ritardo dall'avvenuta conoscenza, di ogni violazione di dati personali (cd. *data breach*), ai sensi degli artt. 33 e 34 del GDPR.

## 5) **Sicurezza dei dati trattati**

Tenuto conto della natura, dell'oggetto, del contesto e delle finalità del trattamento, gli atti con i quali si procede all'affidamento del Registro devono prevedere che l'operatore economico adotti, in qualità di Responsabile, tutte le opportune misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (art. 32 del GDPR) quali, ad esempio:

- (a) misure di «*Business continuity*», che hanno lo scopo di mantenere la continuità delle operazioni essenziali, qualora si verificano situazioni di crisi o incidenti di sicurezza che causino l'indisponibilità dei sistemi per un certo lasso di tempo;
- (b) misure di «*Disaster Recovery*», che garantiscono la capacità di ripristinare i sistemi compromessi nel modo più rapido e sicuro possibile;
- (c) adozione di soluzioni *cloud* rispondenti alla specifica normativa di settore, ivi compresa la disciplina contenuta all'interno del «*Regolamento per le Infrastrutture digitali e per i servizi cloud per la Pubblica Amministrazione, ai sensi dell'articolo 33-septies, comma 4, del Decreto-Legge 18 ottobre 2012, n. 179,*



# *Ministero dell'istruzione e del merito*

*Dipartimento per le risorse, l'organizzazione e l'innovazione digitale*

*Dipartimento per il sistema educativo di istruzione e formazione*

*convertito, con modificazioni, dalla Legge 17 dicembre 2012, n. 211», adottato con Decreto Direttoriale dell'Agencia per la cybersicurezza nazionale n. 21007 del 27 giugno 2024.*

## **6) Trasferibilità dei dati contenuti nel Registro**

I dati contenuti nel Registro devono essere pienamente e facilmente trasferibili ad altri Registri e/o applicazioni rispetto a specifiche esigenze delle Istituzioni scolastiche.