Ministero dell'istruzione e del merito

ALLEGATO B

«*Profili funzionali e tecnici*»

Indice

1. Introduzione 1

2. Descrizione del *Curriculum* e delle tipologie di informazioni e dati personali trattati 1

3. Modalità operative di alimentazione dei dati personali e delle informazioni del *Curriculum* 3

4. Soggetti autorizzati ad accedere 4

5. Operazioni eseguibili sui dati personali e relative modalità di trattamento nell'ambito del *Curriculum* 5

6. Tempistiche di conservazione dei dati personali e delle informazioni nell'ambito di Unica 6

7. Misure di sicurezza tecnico-organizzative per la protezione dei dati personali 7

1. Introduzione

Il presente Allegato B al Decreto descrive i profili funzionali e tecnici afferenti al *Curriculum* e le relative modalità di integrazione, trasmissione e alimentazione dei dati personali e delle informazioni nell'ambito della Piattaforma Unica, nonché le operazioni eseguibili sul *Curriculum* dalle diverse tipologie di utenti (i.e., consultazione ed estrazione), anche con riferimento alle garanzie e alle misure di sicurezza tecnico-organizzative adottate, finalizzate a tutelare i diritti fondamentali dei soggetti i cui dati e informazioni sono coinvolti nel trattamento, in conformità al GDPR, al Codice e agli orientamenti comunitari e nazionali in materia.

2. Descrizione del *Curriculum* e delle tipologie di informazioni e dati personali trattati

Il *Curriculum*, di cui all'Allegato A al Decreto, è reso disponibile nell'ambito della sezione «*Documenti*» del Servizio Digitale *E-Portfolio* dell'area privata della Piattaforma Unica, nel rispetto dei Decreti Unica.

Il *Curriculum* costituisce uno strumento di orientamento funzionale alla restituzione, agli Studenti, del percorso svolto nella globalità dei suoi fattori, attinenti sia all'apprendimento formale sia all'apprendimento non formale.

Il *Curriculum* raccoglie:

a) i dati personali e le informazioni relative a: (*i*) competenze, conoscenze e abilità anche professionali acquisite in ambito scolastico; (*ii*) attività culturali, artistiche e di pratiche musicali, sportive e di volontariato, svolte in ambito extrascolastico; (*iii*) attività svolte nell'ambito dei percorsi per le competenze trasversali;

b) gli esiti e i livelli di apprendimento delle Prove a carattere nazionale, di cui all'articolo 19 del Decreto Legislativo 13 aprile 2017, n. 62, conseguiti in italiano, matematica e inglese, dagli Studenti iscritti all'ultimo anno di scuola secondaria di secondo grado.

I suddetti dati personali e informazioni sono contenuti all'interno delle seguenti parti del *Curriculum*:

- **Parte I - «*Istruzione e formazione*»**, contenente i dati personali e le informazioni relative alla sezione «*Percorso di Studi*» del Servizio *E-Portfolio* di cui alla lettera *(A)*, paragrafo 3 dell'Allegato Tecnico al Decreto Ministeriale 10 ottobre 2023, n. 192;
- **Parte II - «*Certificazioni*»**, contenente le informazioni e i dati personali delle certificazioni conseguite in ambito scolastico, relativi alla sezione «*Sviluppo delle Competenze*» del Servizio *E-Portfolio* di cui alla lettera *(B)*, paragrafo 3 dell'Allegato Tecnico al Decreto Ministeriale 10 ottobre 2023, n. 192;
- **Parte III - «*Attività extrascolastiche*»**, contenente le informazioni e i dati personali delle certificazioni conseguite in ambito extrascolastico, relativi alla sezione «*Sviluppo delle Competenze*» del Servizio *E-Portfolio* di cui alla lettera *(B)*, paragrafo 3 dell'allegato tecnico al Decreto Ministeriale 10 ottobre 2023, n. 192;
- **Parte IV - «*Prove Nazionali*»**, contenente gli esiti e i livelli di apprendimento delle Prove a carattere nazionale, di cui all'articolo 19 del Decreto Legislativo 13 aprile 2017, n. 62, conseguiti in italiano, matematica e inglese, dagli Studenti iscritti all'ultimo anno di scuola secondaria di secondo grado.

Nell'ambito del *Curriculum* sono trattati i soli dati personali comuni degli interessati e non è richiesto il conferimento di dati riconducibili alle categorie particolari di cui agli articoli 9 e 10 del GDPR.

Gli unici dati personali riconducibili all'articolo 9 del GDPR, in quanto potenzialmente idonei a rivelare opinioni politiche, convinzioni religiose o filosofiche, sono quelli desumibili dalle attività e dalle certificazioni conseguite in ambito extrascolastico, che gli Studenti possono inserire volontariamente nella sezione «*Sviluppo delle Competenze*» del Servizio *E-Portfolio* e che sono salvati all'interno della banca dati SIDI, nel rispetto dei Decreti Unica.

Al fine di aumentare il grado di consapevolezza in capo agli Studenti interessati circa il trattamento dei propri dati personali, la Piattaforma:

a) **al momento del primo accesso al Servizio *E-Portfolio***, sottopone agli interessati un'informativa *privacy* descrittiva degli specifici trattamenti connessi al Servizio medesimo, con particolare riferimento ai dati personali e alle informazioni relativi alle attività extrascolastiche, caricate volontariamente dagli Studenti all'interno della Parte III del *Curriculum*;

b) **al momento del primo inserimento delle attività extrascolastiche** all'interno della sezione «*Sviluppo delle Competenze*», sottopone agli interessati uno specifico *alert*, rendendoli edotti circa il rischio, in caso di caricamento di dati riconducibili alle categorie particolari di cui all'articolo 9 del GDPR, dell'eventuale grado di divulgazione cui *Curriculum* può essere soggetto;

c) **al momento dell'acquisizione della Parte III o della versione integrale del *Curriculum*** viene sottoposto allo Studente Diplomato e all'Esercente la responsabilità genitoriale dello Studente Diplomato minorenne uno specifico alert circa la possibile delicatezza dei dati personali contenuti all'interno dei predetti documenti, come previsto nel precedente punto b).

3. Modalità operative di alimentazione dei dati personali e delle informazioni del *Curriculum*

Ai sensi dell'articolo 4 del Decreto, l'alimentazione dei dati personali e delle informazioni nell'ambito del *Curriculum* avviene progressivamente nelle modalità di seguito indicate:

a) **nel corso dell'anno scolastico**, con compilazione, a cura della studentessa e dello studente, della Parte III;

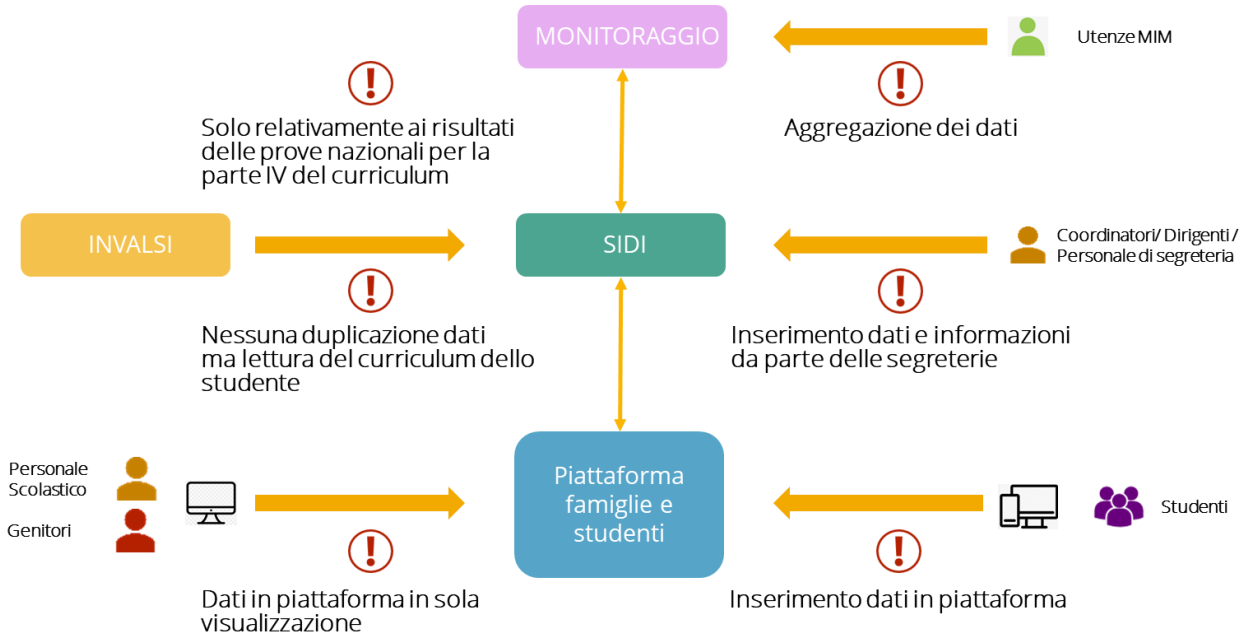
b) **a seguito dello scrutinio finale**, con riferimento alle Parti I (ad eccezione delle informazioni inerenti al titolo di studio e al punteggio finale conseguito), II, III come previsto dal Decreto Ministeriale 6 agosto 2020 n. 88;

c) **all'esito dell'esame di maturità**, con riferimento: (i) alle informazioni inerenti al titolo di studio e al punteggio finale conseguito, che integrano la Parte I; (ii) alla Parte IV.

Per le modalità di integrazione, trasmissione e alimentazione dei dati personali e delle informazioni delle Parti I, II, III, si rimanda a quanto previsto dai Decreti Unica.

I dati personali e le informazioni relativi alla Parte IV, sono (*i*) trasmessi da INVALSI; (*ii*) acquisiti dal sistema SIDI; (*iii*) consultati in Piattaforma.

Tutto ciò premesso, si riporta il nuovo flusso di interazione fra i diversi sistemi coinvolti nell'ambito dell'alimentazione del *Curriculum*, che aggiorna e sostituisce quello del paragrafo 3 dell'allegato tecnico al Decreto Ministeriale del 10 ottobre 2023, n. 192:



4. Soggetti autorizzati ad accedere

Nell'ambito della Piattaforma Unica, l'accesso alle informazioni e ai dati personali contenuti all'interno del *Curriculum* è garantito, previo superamento di una procedura di identificazione e autenticazione informatica secondo le modalità indicate nei Decreti Unica, alle seguenti tipologie di utenti (di seguito, anche «**Utenti**»):

a) Studente Diplomando;

b) Esercente la responsabilità genitoriale dello Studente Diplomando minorenne;

c) Studente Diplomato;

d) Candidati Esterni;

e) docente della scuola secondaria di secondo grado, limitatamente agli Studenti di propria competenza (di seguito, anche «**Docente**»);

f) docente tutor, limitatamente agli Studenti di propria competenza (di seguito, anche «**Docente Tutor**»).

Eseguito l'accesso, gli Utenti visualizzano le informazioni contenute nel *Curriculum* nel rispetto e nei limiti dei seguenti livelli di visualizzazione, di cui all'articolo 5, comma 2, del Decreto:

a) **nel corso dell'anno scolastico**, i dati personali e le informazioni relativi al *Curriculum* sono accessibili alle seguenti categorie di Utenti: (i) Studente Diplomando; (ii) Candidato Esterno; (iii) Esercente la responsabilità genitoriale dello Studente Diplomando minorenne; (iv) Docente; (v) Docente Tutor;

b) **a seguito dello scrutinio finale**, i dati personali e le informazioni relativi al *Curriculum* sono accessibili alle seguenti categorie di Utenti: (i) Studente Diplomando; (ii) Candidato Esterno; (iii) Esercente la responsabilità genitoriale dello Studente Diplomando minorenne;

c) **all'esito dell'esame di maturità**, i dati personali e le informazioni relativi al *Curriculum* sono accessibili alle seguenti categorie di Utenti: (i) Studente Diplomato; (ii) Candidato Esterno; (iii) Esercente la responsabilità genitoriale dello Studente Diplomato minorenne.

Nel rispetto dell'articolo 4, commi 5 e 6, del Decreto, gli Studenti Diplomati e gli Esercenti la responsabilità genitoriale degli Studenti Diplomati minorenni possono, attraverso una scelta informata, acquisire il *Curriculum* nella versione integrale o scaricando le sezioni del documento nelle seguenti versioni:

a) versione comprensiva delle Parti I e II;

b) versione comprensiva delle Parti I, II e III;

c) versione comprensiva della sola parte IV, sezione autonoma e separata.

Nel caso in cui lo studente e la studentessa acquisiscano la versione integrale del *Curriculum* o la versione di cui alla precedente lettera b), la Piattaforma sottopone uno specifico alert circa i rischi in materia di protezione dei dati personali, come previsto nel precedente paragrafo 2.

5. Operazioni eseguibili sui dati personali e relative modalità di trattamento nell'ambito del *Curriculum*

Le operazioni eseguibili sui dati personali e sulle informazioni contenute nell'ambito del *Curriculum* e i soggetti autorizzati a eseguire le medesime operazioni sono indicate nella tabella sottostante:

PERIODO DI RIFERIMENTO	TIPOLOGIA DI DATI PERSONALI E INFORMAZIONI	SOGGETTI AUTORIZZATI E OPERAZIONI ESEGUIBILI
nel corso dell'anno scolastico	Dati personali e informazioni contenute nelle Parti III.	▪ Studente Diplomando: - caricamento; - consultazione; - estrazione (download). ▪ Candidato Esterno: - caricamento; - consultazione; - estrazione (download). ▪ Esercente la responsabilità genitoriale dello Studente minorenne: - consultazione: - estrazione (download). ▪ Docente/ Docente Tutor: - consultazione; - estrazione (download).
a seguito dello scrutinio finale	Dati personali e informazioni contenute nelle Parti I (ad eccezione delle informazioni inerenti al titolo di studio e al punteggio finale conseguito), II, III come previsto dal Decreto Ministeriale 6 agosto 2020 n. 88.	▪ Studente Diplomando: - consultazione; - estrazione (download). ▪ Candidato Esterno: - consultazione; - estrazione (download). ▪ Esercente la responsabilità genitoriale dello Studente Diplomato minorenne:

PERIODO DI RIFERIMENTO	TIPOLOGIA DI DATI PERSONALI E INFORMAZIONI	SOGGETTI AUTORIZZATI E OPERAZIONI ESEGUIBILI
		- consultazione: - estrazione (download).
all'esito dell'esame di maturità	Dati personali e informazioni contenute nelle Parti I, incluse le informazioni inerenti al titolo di studio e al punteggio finale conseguito, II, III e IV (cfr. articolo 21 del Decreto Legislativo del 13 aprile 2017, n. 62, come da ultimo modificato dall'articolo 14, comma 6, del Decreto-Legge del 2 marzo 2024, n. 19, convertito con modificazioni dalla Legge del 29 aprile 2024, n. 56).	▪ Studente Diplomato: - consultazione: - estrazione (download). ▪ Candidato Esterno diplomato: - consultazione; - estrazione (download). ▪ Esercente la responsabilità genitoriale dello Studente Diplomato minorenne: - consultazione; - estrazione (download).

(*Tabella 1- Modalità di trattamento nell'ambito del Curriculum*)

6. Tempistiche di conservazione dei dati personali e delle informazioni nell'ambito di Unica

I dati personali che la Piattaforma Unica acquisisce da banche dati preesistenti non sono oggetto di conservazione nell'ambito della Piattaforma medesima.

In particolare, nel rispetto del principio di limitazione della conservazione di cui al GDPR, i codici fiscali degli Studenti Diplomati e degli Esercenti la responsabilità genitoriale degli Studenti minorenni Diplomati, necessari ai fini della procedura di identificazione e autenticazione alla Piattaforma Unica, sono conservati per il periodo di tempo necessario ai fini degli accertamenti di legge e, in particolare, 1 (uno) anno decorrente dal conseguimento del diploma, e saranno conservati all'interno di una apposita banca dati della Piattaforma Unica, nel rispetto dei Decreti Unica.

È altresì oggetto di oggetto di conservazione, all'interno della predetta banca dati, l'informazione relativa all'avvenuta presa visione da parte dell'Esercente la responsabilità genitoriale delle Prove a carattere nazionale nell'ambito Servizio Digitale *E-Portfolio*.

7. Misure di sicurezza tecnico-organizzative per la protezione dei dati personali

Il Ministero dell'Istruzione e del Merito ha nominato quale Responsabile del trattamento dei dati personali, ai sensi dell'articolo 28 del GDPR, la Sogei S.p.A., in quanto affidataria dei servizi infrastrutturali, di gestione e sviluppo applicativo del sistema informativo del Ministero medesimo.

Il Ministero, attraverso apposite istruzioni operative, ha richiesto alla Sogei di operare attenendosi alle previsioni contenute nel documento condiviso di «*Metodologia per la protezione dei dati e per la valutazione d'impatto*».

In adempimento all'articolo 32 del GDPR il Responsabile ha adottato sulle sue infrastrutture tecnologiche le seguenti misure di sicurezza infrastrutturali, oltre a quelle risultanti dalle valutazioni di impatto:

NOME MISURA	DESCRIZIONE MISURA
Manutenzione da remoto delle apparecchiature	In caso di interventi di manutenzione di apparecchiature interne (es. data storage) effettuati da remoto dall'esterno della sede Sogei: - viene aperto il canale solo per il tempo di connessione necessario all'intervento; - vengono tracciate le operazioni svolte dal tecnico esterno insieme al motivo dell'accesso; - viene utilizzato un canale di comunicazione cifrato.
Autenticazione, memorizzazione e trasmissione credenziali	Il sistema di controllo accessi prevede che le credenziali di autenticazione siano trasmesse in forma cifrata (cifratura delle credenziali e/o del canale) su reti non fidate.
Controllo accessi, utenze di servizio	Le utenze di servizio applicative (ovvero utenze utilizzate dalle applicazioni per connettersi alle basi dati o per richiamare altre applicazioni) non sono utilizzate per effettuare login interattivi allo scopo di accedere direttamente ai dati.
Vulnerabilità tecniche, protezione sistemi in produzione	I sistemi in produzione sono protetti tramite apparati che garantiscono: - la separazione delle reti (reti demilitarizzate) e il controllo del traffico consentito tramite firewall; - la protezione da attacchi informatici condotti mediante i protocolli di rete consentiti (controlli Deep Packet Inspection con sonde IPS, antivirus di rete, anti-botnet, anti ddoS).

Vulnerabilità tecniche, svolgimento attività	Le attività di verifica delle vulnerabilità tecniche (vulnerability assessment) di un servizio ICT: - vengono svolte attraverso strumenti sempre aggiornati rispetto agli ultimi vettori di attacco scoperti; - seguono specifici test-plan definiti in base alla documentazione di progetto e alla tipologia di piattaforma; - vengono pianificate in funzione della criticità dei sistemi impattati; - sono oggettive, ripetibili e conformi a standard di riferimento.
Integrità dei log degli ADS e degli incaricati	I log del servizio ICT e i log di accesso degli Amministratori di sistema e degli incaricati sono protetti da eventuali tentativi di alterazione ed è possibile verificarne l'integrità.
Capacità dei servizi, monitoraggio	Il servizio ICT è sottoposto a monitoraggio continuo della capacità attraverso l'analisi dei seguenti parametri: - performance della rete (utilizzo della banda); - livelli di carico delle macchine; - utilizzo della CPU; - occupazione della RAM; - occupazione del file system; - spazio disco utilizzato e disponibile.
Capacità dei servizi, piano di adeguamento	Laddove si renda necessario un adeguamento di capacità dell'infrastruttura tecnologica a supporto del servizio ICT viene redatto un piano di adeguamento tecnologico che contiene: - l'analisi effettuata sul monitoraggio del servizio; - le variazioni da implementare per raggiungere i risultati desiderati e i componenti dell'infrastruttura interessati; - l'orizzonte temporale in cui effettuare le modifiche.
Capacità dei servizi, adeguamento	L'adeguamento di capacità dell'infrastruttura tecnologica su cui si basa il servizio ICT è soggetto alle procedure di change management aziendali per tenere traccia di tutte le richieste di variazione. Tutte le componenti hardware/software del servizio sono censite su CMDB.

Gestione eventi/incidenti, workflow	Le procedure per la gestione degli eventi/incidenti di sicurezza sono automatizzate o supportate da strumenti informatici che ne gestiscono il workflow, tracciano le operazioni svolte, conservano le evidenze e supportano l'analisi.
Monitoraggio allarmi	Le segnalazioni e gli allarmi provenienti dall'infrastruttura di rete, dai server e dalle postazioni client sono soggetti a monitoraggio per individuare eventuali anomalie.
Gestione eventi, correlazione	Gli eventi di sicurezza segnalati e rilevati sono analizzati e correlati tra loro al fine di stabilirne la gravità e identificare eventuali incidenti di sicurezza.
Repository di supporto per la gestione degli incidenti	Viene utilizzato e regolarmente aggiornato un repository di supporto per la risoluzione degli incidenti di sicurezza che contiene la descrizione del problema riscontrato, le attività intraprese, i workaround e le soluzioni implementate.
Inventario servizi applicativi	Si utilizzano strumenti di asset management (Catalogo dei servizi, Information Governance, CMDB) al fine di creare un inventario e correlare il servizio applicativo ai dati e ai relativi componenti software e hardware.
Tracciamento operazioni effettuate sulle basi dati	Per ogni accesso alle basi dati ospitate presso i CED Sogei, effettuato tramite utenze nominali o riconducibili ad una persona fisica (escluse le utenze di servizio), il sistema di tracciamento registra le seguenti informazioni (log): - identificativo univoco dell'utenza che accede - data e ora di login, logout e login falliti - postazione di lavoro utilizzata per l'accesso - tipo di operazione eseguita sui dati (ad esclusione delle risposte alle query).
Tracciamento dei sistemi di sicurezza di rete	I sistemi di sicurezza di rete (firewall, intrusion prevention, …) tracciano gli eventi e le eventuali anomalie connesse ad essi al fine di individuare eventuali attacchi informatici o diffusione di malware.
Tracciamento, generazione di report	Il sistema di tracciamento permette la generazione di report e la loro esportazione in formati che consentono di analizzarli.

Tracciamento, sincronizzazione degli orologi	Gli orologi dei sistemi tracciati sono sincronizzati con una fonte temporale autoritativa.
Tracciamento, monitoraggio dei file di log di sistema	I log prodotti dai sistemi di tracciamento infrastrutturali sono soggetti a monitoraggio allo scopo di individuare eventuali anomalie inerenti alla sicurezza (accessi anomali, operazioni anomale, ecc.) e di valutare l'efficacia delle misure implementate.
Backup	Il backup delle componenti del servizio ICT (configurazioni, software applicativo, file di log, back-end App, dati) viene eseguito in maniera incrementale con cadenza giornaliera e completa con cadenza settimanale. In caso di danneggiamento, il processo di ripristino viene attivato entro otto ore. I tempi di ripristino dipendono dal volume dei dati da ripristinare.

Firmato digitalmente da VALDITARA GIUSEPPE
C=IT
O=MINISTERO DELL'ISTRUZIONE E DEL MERITO