VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

ai sensi del GDPR 2016/679 e normativa nazionale in vigore

Organizzazione: **Direzione Didattica Statale 1° Circolo di Quarto**

SEDE	**Direzione Didattica Statale 1° Circolo di Quarto** **Via Primo Maggio 4** **80010 - Quarto (NA)** **tel: 081 8761777** **email: naee17300n@istruzione.it** **pec: naee17300n@pec.istruzione.it** **Cod. Fisc. 80029800630** **Sito Web: www.primocircoloquarto.edu.it**

Data revisione: 08/10/2022

SOMMARIO

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI

La DPIA, acronimo di Data Protection Impact Assessment, è una valutazione preliminare, eseguita dal titolare del trattamento dei dati personali, relativa agli impatti a cui andrebbe incontro un trattamento laddove dovessero essere violate le misure di protezione dei dati.

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento; è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35 del Regolamento 2016/679).

OBBLIGO DPIA

Ai sensi dell'articolo 35, paragrafo 3 del Regolamento 2016/679 la valutazione è stata effettuata nei casi in cui un trattamento può presentare rischi elevati, ossia quando:

a. una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b. il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10;
c. la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

CRITERI DA CONSIDERARE PER OBBLIGO DPIA

Nel percorso di analisi sono stati presi in considerazione i seguenti 9 criteri:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Nel caso in cui un'attività di trattamento dati soddisfa due o più criteri viene eseguita la valutazione d'impatto sulla protezione dei dati.

REVISIONE

Secondo le buone prassi, la valutazione d'impatto sulla protezione dei dati viene riesaminata continuamente e rivalutata con regolarità.

ALGORITMO VALUTAZIONE

1° STEP: IDENTIFICAZIONE DEI TRATTAMENTI

Il primo step consiste nel censire tutte le attività di trattamento di dati personali specificandone:

- dati identificativi (Sede, struttura, funzioni),
- finalità,
- tipologia di dati personali trattati,
- categorie di interessati,
- destinatari,
- modalità di elaborazione dati (cartacea, elettronica, mista),
- termine cancellazione dati,
- eventuale trasferimento paesi terzi,
- misure di sicurezza.

2° STEP: VALUTAZIONE DEL RISCHIO E INDIVIDUAZIONE CRITERI PER DPIA

Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. L'entità dei rischi viene ricavata assegnando un opportuno valore alla **probabilità di accadimento (P)** ed alle **conseguenze** di tale evento **(C)**. Dalla combinazione di tali grandezze si ricava la matrice di rischio la cui entità è data dalla relazione:

LR = P X C

LR = livello di rischio

P = probabilità di accadimento

C = conseguenze

Alla **probabilità di accadimento dell'evento P** è associato un indice numerico rappresentato nella seguente tabella:

PROBABILITA' DELL'EVENTO	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**M. Probabile**
5	**Quasi certo**

Alle **Conseguenze** (C) è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**
5	**Gravissime**

MATRICE DEI RISCHI

La matrice che scaturisce dalla combinazione di **probabilità** e **conseguenze** è rappresentata in figura seguente:

Probabilità						
	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	**2**	**3**	**4**	**5**
		Conseguenze				

Entità Rischio	Valori di riferimento
Accettabile	*(1 ≤ **LR** ≤ 3)*
Medio - basso	*(4 ≤ **LR** ≤ 6)*
Rilevante	*(8 ≤ **LR** ≤ 12)*
Alto	*(15 ≤ **LR** ≤ 25)*

Si ricava, così, per ogni attività di trattamento un Livello di Rischio (di potenziale perdita, divulgazione, modifica, distruzione non autorizzata di dati).

In questo step viene anche ricercata la presenza di criteri di obbligo DPIA:

1. Valutazione o assegnazione di un punteggio
2. Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente
3. Monitoraggio sistematico
4. Dati sensibili o aventi carattere altamente personale
5. Trattamento di dati su larga scala
6. Creazione di corrispondenze o combinazione di insieme di dati
7. Dati relativi ad interessati vulnerabili
8. Uso innovativo o applicazione di nuove soluzioni tecnologiche
9. Trattamento che impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto

Se vi è presenza di almeno due criteri e/o il Livello di Rischio risulta ALTO, l'attività richiede la DPIA.

3 STEP: DPIA – VALUTAZIONE DEL RISCHIO NORMALIZZATO

Ai sensi dell'art. 35 del GDPR, vengono individuate tutte le attività di trattamento che in prima analisi presentano un livello di rischio alto e/o prevendono due o più criteri di obbligo DPIA.

Nel caso in cui, quindi, l'indice di rischio si colloca nel range 15 ÷ 25, l'attività necessita di una valutazione di impatto mediante un'analisi approfondita di alcuni aspetti.

La DPIA si basa su un'analisi dei rischi più dettagliata cercando di dare un peso ai possibili controlli applicabili, ricavando, così, un indice di rischio "normalizzato" rispetto al contesto aziendale.

Il rischio viene calcolato in funzione dei 3 fattori seguenti:

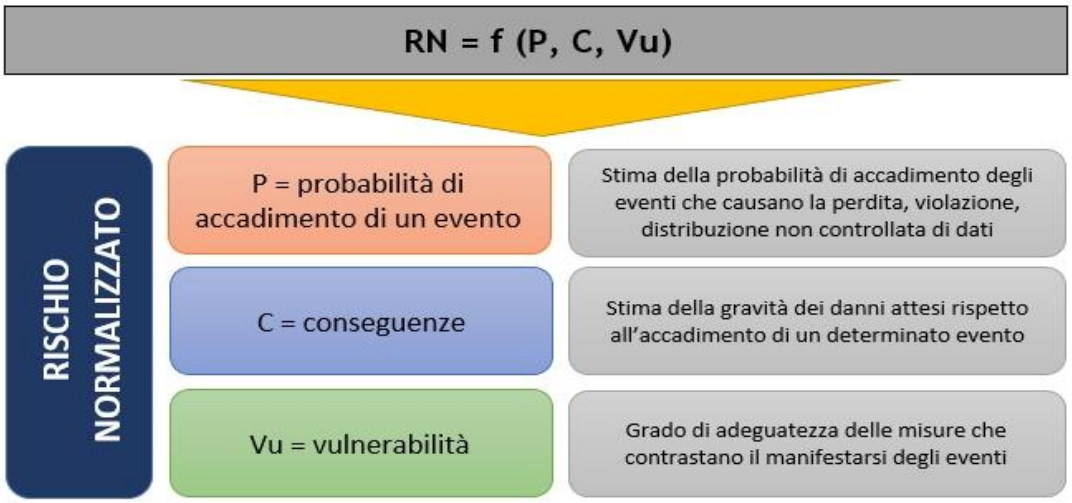
RN = f (P, C, Vu)

Dove:

P = probabilità

C = conseguenze generate dall'evento

V = vulnerabilità rispetto al grado di adeguatezza delle misure



In prima battuta viene ricavato il **Rischio intrinseco** (**Ri)** come prodotto della **probabilità (P)** e delle **Conseguenze (C)**, in base agli indici numerici assegnati ad entrambi i fattori.

Alla **Probabilità (P)** è associato un indice numerico rappresentato nella seguente tabella:

Probabilità	
1	**Improbabile**
2	**Poco probabile**
3	**Probabile**
4	**Quasi certo**

Alle **Conseguenze (C)** è associato un indice numerico rappresentato nella seguente tabella:

CONSEGUENZE	
1	**Trascurabili**
2	**Marginali**
3	**Limitate**
4	**Gravi**

Rispetto al 1 STEP, la matrice ha un range ridotto, essendo una matrice 4 x 4:

PROBABILITÀ	4	4	8	12	16
	3	3	6	9	12
	2	2	4	6	8
	1	1	2	3	4
		1	2	3	4
		CONSEGUENZE			

RISCHIO INTRINSECO	
Ri = P x C	**Valori di riferimento**
Molto basso	*(1 ≤ **Ri** ≤ 2)*
Basso	*(3 ≤ **Ri** ≤ 4)*
Rilevante	*(6 ≤ **Ri** ≤ 9)*
Alto	*(12 ≤ **Ri** ≤ 16)*

Il rischio intrinseco viene ricavato prendendo in considerazione tutti i possibili Pericoli e Rischi.

Per ricavare il **Rischio Normalizzato RN**, viene introdotto il fattore Vulnerabilità Vu che fornisce un'indicazione circa l'adeguatezza delle misure di sicurezza attuate per ogni rischio.

Alla **Vulnerabilità** (**Vu**) è associato un indice numerico rappresentato nella seguente tabella:

	VULNERABILITA'	**Valore**
1	**Adeguate**	**0,25**
2	**Parzialmente adeguate**	**0,5**
3	**Inadeguate**	**1**

Per ogni rischio vengono indicate le misure di sicurezza adottate, per ognuna delle quali viene definito il grado di adeguatezza, assegnando uno dei possibili valori:

- 0,25;
- 0,5;
- 1.

Per ricavare il valore del rischio normalizzato RN viene moltiplicato il Rischio Intrinseco Ri con il valore peggiore assegnato alle misure di sicurezza relativamente a quel rischio.

Vu	1	$1 < RN \leq 2$	$3 \leq RN \leq 4$	$6 \leq RN \leq 9$	$12 \leq RN \leq 16$
	0,5	$0,5 < RN \leq 1$	$1,5 \leq RN \leq 2$	$3 < RN \leq 5$	$6 \leq RN \leq 8$
	0,25	$0,25 \leq RN \leq 0,5$	$0,75 \leq RN \leq 1$	$1,5 \leq RN < 3$	$3 \leq RN \leq 4$
		$1 \leq Ri \leq 2$	$3 \leq Ri \leq 4$	$6 \leq Ri \leq 9$	$12 \leq Ri \leq 16$
		Ri			

RISCHIO NORMALIZZATO	
RN = Ri x Vu	**Valori di riferimento**
Molto basso	$0,25 \leq RN \leq 1$
Basso	$1 < RN < 3$
Rilevante	$3 \leq RN \leq 9$
Alto	$12 \leq RN \leq 16$

Se, a valle dell'analisi DPIA, l'attività ricade comunque in fascia ALTA, il Titolare attiva l'iter di consultazione del Garante

RISULTATI DPIA

Di seguito, viene riportata l'analisi di tutte le attività di trattamento per cui si è resa necessaria la valutazione di impatto sulla protezione dei dati.

Elenco attività sottoposte a DPIA:

- *Attività di Didattica a Distanza*

ATTIVITÀ DI DIDATTICA A DISTANZA

TRATTAMENTO: Dati relativi alla didattica a distanza (DAD)

Struttura	• **Sede legale** • **Sedi operative**

Personale coinvolto	
Persone autorizzate	Direzione Didattica Statale 1° Circolo di Quarto nella persona della **Prof.ssa Stefania Albiani** (Rappresentante legale), Docenti, **Amministratori di Sistema** Attività: • Cancellazione • Comunicazione • Conservazione • Consultazione • Distribuzione • Elaborazione • Organizzazione • Raccolta

Processo di trattamento	
Descrizione	Secondo le disposizioni del D.L. n°6 del 23 febbraio 2020, del D.P.C.M. del 8 marzo 2020, delle note del Ministero dell'Istruzione del 6 marzo 2020, prot. n. 278, e dell'8 marzo 2020, prot. n. 279, con le quali sono state fornite istruzioni operative alle istituzioni scolastiche sull'attivazione e sul potenziamento di modalità di apprendimento a distanza, ottimizzando le risorse didattiche del registro elettronico e utilizzando classi virtuali, ovvero altri strumenti e canali digitali, per favorire la

	produzione e la condivisione di contenuti; della nota del Ministero dell'Istruzione del 17 marzo 2020, prot. n. 388, nella quale sono state fornite, tra l'altro, alcune indicazioni sulla protezione dei dati personali trattati nell'ambito della didattica a distanza; della Dichiarazione sul trattamento dei dati personali nel contesto dell'epidemia di COVID-19, adottata dal Comitato europeo per la protezione dei dati (EDPB) in data 19 marzo 2020, in rispetto ai contenuti del Provvedimento del Garante della Privacy n°64 del 26 marzo 2020, del Decreto Legislativo 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali") nel seguito indicato sinteticamente come Codice, e del GDPR 2016/679, nel seguito indicato sinteticamente come GDPR, si forniscono i dettagli sul trattamento e sulla gestione dei dati personali specificatamente per ciò che riguarda l'attività della didattica a distanza (DAD). I dati personali dell'utente saranno utilizzati dall'Istituzione scolastica, che ne è titolare per il trattamento, nel rispetto dei principi di protezione dei dati personali stabiliti dalla normativa in vigore.
Fonte dei dati personali	Raccolti direttamente Forniti da terzi
Base giuridica per il trattamento per dati comuni (art. 6 GDPR)	La nota MIUR m_pi.AOODPIT.REGISTRO UFFICIALE(U).0000388.17-03-2020 specifica *"Occorre subito precisare che le istituzioni scolastiche non devono richiedere il consenso per effettuare il trattamento dei dati personali (già rilasciato al momento dell'iscrizione) connessi allo svolgimento del loro compito istituzionale, quale la didattica, sia pure in modalità "virtuale" e non nell'ambiente fisico della classe. Le istituzioni scolastiche sono invece tenute, qualora non lo abbiano già fatto, ad informare gli interessati del trattamento secondo quanto previsto dagli artt. 13 e 14 del Regolamento UE 2016/679"*. Sulla scorta di quanto riportato, non è necessario il consenso da parte delle famiglie. Il Garante privacy ribadisce, nel comunicato del 30 marzo e nelle indicazioni collegate, che "Le scuole e le università che utilizzano sistemi di didattica a distanza non devono richiedere il consenso al trattamento dei dati di docenti, alunni, studenti, genitori, poiché il trattamento è riconducibile alle funzioni istituzionalmente assegnate a scuole e atenei". Il Dirigente scolastico fornisce agli interessati l'Informativa sul trattamento dati, che gli stessi devono visionare e, nel caso dovessero riscontrare elementi di inadeguatezza o poco chiari, possono manifestare le proprie osservazioni, chiedere chiarimenti, esercitare i propri diritti comunicando alla scuola attraverso i contatti ufficiali
Base giuridica per il trattamento per dati particolari (art. 9 GDPR)	I dati personali definiti come "dati particolari" dal Codice e i dati previsti dagli art.9 e 10 del GDPR sono trattati esclusivamente dal personale della scuola, appositamente incaricato, secondo quanto previsto dalle disposizioni di legge e nel rispetto del principio di stretta indispensabilità dei trattamenti. Gli eventuali dati particolari veicolati sul registro elettronico o su piattaforme DAD non saranno oggetto di diffusione alcuna (si cercherà comunque di trovare soluzioni, insieme con i genitori degli interessati che possano consentire che tali dati veicolino solo su applicativi con identificazione certa del ricevente). Saranno sempre rispettate le adeguate misure per salvaguardare la tutela dei minori in ogni loro aspetto (così come previsto dalla Carta di Treviso del 5 ottobre 1990 e

	successive integrazioni e dal D.P.R. 24 giugno 1998, n. 249, spec. art. 1; art. 13 del Regolamento). Il trattamento DAD sarà effettuato con strumenti elettronici, nel rispetto delle misure di sicurezza indicate dal Codice e delle altre individuate ai sensi del Regolamento e dal già citato Provvedimento del Garante. I dati verranno conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID. Saranno rispettati i presupposti e le condizioni per il legittimo impiego di strumenti tecnologici nel contesto lavorativo (artt. 5 e 88, par. 2, del GDPR, art. 114 del Codice e dell'art. 4 della legge 20 maggio 1970, n. 300) limitandosi a utilizzare quelli strettamente necessari, comunque senza effettuare indagini sulla sfera privata (art. 113 del citato Codice) o interferire con la libertà di insegnamento.
Finalità del trattamento	Il trattamento nell'ambito della DAD è riconducibile alle funzioni istituzionalmente ad esse assegnate. Il trattamento dei dati personali degli alunni che frequentano l'istituto scolastico ha come finalità esclusive la gestione della DAD (didattica a distanza) per compensare la sospensione delle attività didattiche e dei servizi educativi delle scuole di ogni ordine e grado, previste tra le misure adottate dal Presidente del Consiglio per il contenimento dell'emergenza epidemiologica. È garantito il rispetto del senso di responsabilità che investe gli operatori della scuola nel garantire una continuità didattica a tutti i suoi studenti. In forza di ciò, il titolare del trattamento ha deciso di attivare un sistema di Didattica a Distanza per far fronte all'attuale situazione. I dati veicolati sugli applicativi scelti saranno trattati, per ciò che compete l'istituzione scolastica (per esempio elaborati degli alunni), in maniera strettamente necessaria all'assolvimento degli obblighi educativi; trattati in modo lecito e corretto; pertinenti alle finalità della raccolta e del successivo trattamento; conservati per un periodo di tempo limitato e, comunque, non superiore al periodo necessario allo scopo per cui sono stati raccolti. Ogni utente provvederà singolarmente a generare il proprio account per accedere alla DAD, di conseguenza l'istituto scolastico non conserverà nessun dato riconducibile allo stesso utente.
Tipo di dati personali	I dati personali di ogni alunno sono stati già conferiti all'atto dell'iscrizione direttamente dal genitore, o dalle scuole di provenienza. Il trattamento è effettuato secondo i principi di liceità, correttezza e trasparenza nei confronti dell'interessato e trattati compatibilmente con le finalità del trattamento. I dati raccolti sono minimizzati, cioè adeguati, pertinenti e limitati a quanto strettamente necessario rispetto alle finalità del trattamento. La raccolta di eventuali dati fotografici/video/audio, da parte dei singoli docenti, è limitata a casi estremamente eccezionali e dopo aver acquisito l'approvazione scritta preliminare del titolare del trattamento e del responsabile interno del trattamento. Il trattamento viene effettuato prevalentemente all'interno dell'istituto scolastico, oltre che dal dirigente scolastico, anche dal personale dipendente autorizzato al trattamento in relazione alle mansioni istituzionali ricoperte (DSGA, ATA amministrativi, Organi collegiali, Docenti). Trattamenti relativi alla DAD sono effettuati in esterno, in via prioritaria dal fornitore della piattaforma che gestisce il registro elettronico, sono utilizzate anche piattaforme di conference call finalizzate alle video lezioni gestite da fornitori esterni sempre nei

	limiti stabiliti dal GDPR e dal Provvedimento del Garante n°64 del 26 marzo 2020. Il trattamento di dati svolto dai fornitori esterni della DAD per conto della scuola si limiterà a quanto strettamente necessario alla fornitura dei servizi richiesti ai fini della didattica on line e non per ulteriori finalità proprie del fornitore. Tali servizi on line sono forniti direttamente agli utenti, con funzionalità di videoconferenza ad accesso riservato senza la necessaria creazione di un account da parte degli utenti. Il fornitore esterno fornirà esclusivamente il servizio on line di videoconferenza tramite la quale non viene effettuato il monitoraggio sistematico degli utenti, o, comunque, non ricorre a nuove soluzioni tecnologiche particolarmente invasive (quali, tra le altre, quelle che comportano nuove forme di utilizzo dei dati di geolocalizzazione o biometrici). L'eventuale trattamento ulteriore dei dati degli utenti, effettuata direttamente dai gestori dei servizi on line, nella diversa veste di titolari del trattamento, dovrà naturalmente osservare, tra gli altri, gli obblighi di informazione e trasparenza secondo quanto previsto dall'art. 13 del GDPR. In caso di eventuali trattamenti non previsti derivanti da attivazione di servizi attualmente non gestiti, e prima della loro attivazione, si provvederà a fornire all'interessato specifica informativa necessaria a tali diverse finalità. Il complesso processo di trattamento DAD, riferibile all'istituto scolastico, viene controllato dalla fase di raccolta fino all'archiviazione storica mantenuta per i periodi stabili dalla normativa attualmente in vigore.
Categorie di interessati	Alunni, Docenti
Categorie di destinatari	Docenti, Responsabile della piattaforma DAD
Informativa	Si
Profilazione	Non presente
Dati particolari	Si
Consenso minori	Non necessario
Frequenza trattamento	Durante il periodo previsto per la DAD
Termine cancellazione dati	I dati obbligatori ai fini della gestione degli alunni e del loro percorso di studi sono conservati per il tempo stabilito dalla normativa in vigore. I dati non più ritenuti utili, saranno immediatamente cancellati o trattati in forma anonima, ove la loro conservazione non risulti altrimenti giustificata da norma di legge.
Trasferimento dati (paesi terzi)	Probabile

Modalità di elaborazione dati: elettronica	
Strumenti	Piattaforma che gestisce il registro elettronico, piattaforme di conference call finalizzate alle video lezioni gestite da fornitori esterni, piattaforme per la didattica on line
Archiviazione	I dati verranno conservati secondo le indicazioni delle Regole tecniche in materia di conservazione digitale degli atti definite da AGID.

Strutture informatiche di archiviazione
Server interno all'Istituzione scolastica e server utilizzati dalle aziende che forniscono i servizi associati alla Didattica a Distanza

MAPPA DATI – ACCESSI

Di seguito è riportata una mappa con i destinatari (audience) che hanno la possibilità di visionare diverse tipologie di dati personali e quali dati personali sono utilizzati all'interno della piattaforma:

Dati personali / **Audience**	**Studenti**	**Docenti**	**Amministratori di Sistema**
Nominativo	✓	✓	✓
Nome utente	✓	✓	✓
Data di nascita	×	×	✓
Classe	Soltanto la propria	Soltanto le assegnate	✓
Valutazioni	Soltanto le proprie	Soltanto le classi assegnate	✓
e-mail	✓	✓	✓
File personali	Solo i condivisi	Solo i condivisi	✓
Riprese in conference	✓	✓	✓

TIPOLOGIE DI TRATTAMENTO CHE RAPPRESENTANO UN RISCHIO ELEVATO

1 - Valutazione di profilazione o scoring	Tutti quei trattamenti che analizzano i dati presenti all'interno dei propri archivi allo scopo di trarne informazioni riguardo il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti dell'interessato
2 - Decisioni automatizzate	Tutti quei trattamenti che producano effetti giuridici sulla persona fisica ovvero che incidono in modo analogo significativamente su dette persone fisiche
3 - Monitoraggio sistematico	Tutti quei trattamenti che sono utilizzati per osservare, monitorare o controllare gli interessati, compresa la raccolta di dati attraverso reti o la sorveglianza di un'area accessibile al pubblico

4 - Dati sensibili o estremamente personali	Tutti quei trattamenti che si riferiscono a particolari categorie di dati sensibili o estremamente personali
5 - Dati trattati su larga scala	Tutti i trattamenti che gestiscono dati personali su larga scala, in relazione al numero di soggetti interessati, al volume dei dati, alla durata o all'ambito geografico
6 - Combinazioni o raffronto di insieme di dati	Tutti quei trattamenti nei quali è prevista una presenza congiunta di due o più titolari distinti, secondo modalità che esulano dalle ragionevoli aspettative dell'interessato
7 - Dati relativi a interessati vulnerabili	Tutti quei trattamenti in cui la tipologia delle informazioni trattate determina uno squilibrio fra interessato e titolare, nel senso della mancanza del potere, in capo al primo, di acconsentire o di opporsi al trattamento. Si inseriscono in questa categoria i dati dei minori, dei dipendenti o delle persone richiedenti specifiche tutele
8 - Utilizzi innovativi	Tutti quei trattamenti che utilizzano tecnologie o tecniche innovative per la raccolta o l'utilizzo dei dati personali, dato che il livello di conoscenza tecnologica, in un dato momento storico, non è in grado valutare il livello di rischio connesso all'innovazione
9 - Trattamenti che impediscono di esercitare un diritto o avvalersi di un servizio o contratto	Tutti quei trattamenti che impediscono agli interessati di esercitare un diritto di avvalersi di un servizio o di un contratto, ossia tutti i trattamenti dai quali l'interessato non può esimersi qualora volesse accedere a detto servizio o concludere detto contratto

MOTIVO DELLA REDAZIONE DPIA

MOTIVO DELLA REDAZIONE DPIA	
1 - Valutazione di profilazione o scoring	✓
2 - Decisioni automatizzate	×
3 - Monitoraggio sistematico	✓
4 - Dati sensibili o estremamente personali	×
5 - Dati trattati su larga scala	✓
6 - Combinazioni o raffronto di insieme di dati	✓
7 - Dati relativi a interessati vulnerabili	×
8 - Utilizzi innovativi	✓
9 - Trattamenti che impediscono di esercitare un diritto o avvalersi di un servizio o contratto	✓

RISCHI
1. Accesso illegittimo ai dati 2. Modifiche non autorizzate dei dati 3. Perdita dei dati 4. Diffusione non autorizzata di dati 5. Accesso non autorizzato alle sessioni in conference call 6. Profilazione degli utenti da parte del gestore della piattaforma 7. Lock-in e fidelizzazione degli utenti 8. Utilizzo dell'account della piattaforma per il tracciamento da parte dei motori in attività extra scolastiche 9. Esportazione dati in paesi extra UE con norme e sensibilità non allineate ai principi del GDPR 10. Retention non definita e non legata con la semplice cancellazione dei dati da parte degli utenti

MISURE DI SICUREZZA TECNICHE ED ORGANIZZATIVE

A. I sistemi di autorizzazione prevedono: la presenza di diversi profili di autorizzazione, l'individuazione preventiva per incaricato, l'individuazione preventiva per classi omogenee di incaricati, la verifica almeno annuale dei profili

B. Sono definiti i ruoli e le responsabilità

C. Sono gestiti i backup

D. Sono utilizzati software antivirus e anti intrusione

E. Crittografia utilizzata per la conservazione e la comunicazione dei dati

F. Controllo degli accessi logici

G. Minimizzazione dei dati

H. Contratto con il responsabile del trattamento

I. Gestione degli incidenti di sicurezza e violazioni dei dati personali attraverso l'adozione di una procedura per la gestione dei data breach

J. Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti.

K. Formazione agli utenti sull'utilizzo dei prodotti "gratuiti" e sul tema della cybersecurity.

L. Formazione sul tema della cyberbullismo.

M. Clausole contrattuali con il fornitore

N. Informative e consenso specifico per gli utenti

ACCESSO ILLEGITTIMO AI DATI

RISCHIO		
Accesso illegittimo ai dati		
POTENZIALE IMPATTO		
Diffusione di informazioni anche sensibili con potenziale impatto sulla dignità e libertà degli interessati. Data Breach. Diffusione di dati personali di minori, diffusione di dati concernenti l'orientamento politico, la razza o la condizione sanitaria degli interessati, Cyberbullismo. Pubblicazione su piattaforme social di dati personali, Scarsa sensibilità degli studenti alla privacy dei compagni, negazione del diritto all'oblio.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Precise disposizioni e prescrizioni sull'utilizzo della piattaforma. Formazione sul tema della cybersecurity. Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti. Tutte le misure esistenti o pianificate individuate.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Poco probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Rilevante	Adeguate (0,25)	Basso

MODIFICHE NON AUTORIZZATE DEI DATI

RISCHIO		
Modifiche non autorizzate dei dati		
POTENZIALE IMPATTO		
La violazione potrebbe portare ad una errata valutazione dell'alunno.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica. Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti. Tutte le misure esistenti o pianificate individuate.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Limitate	Accettabile
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Molto basso	Adeguate (0,25)	Molto basso

RISCHIO		
Perdita di dati a causa di azioni volontarie o non ed agenti fisici (incendi, allagamenti, attacchi esterni, ecc.)		
POTENZIALE IMPATTO		
Possibile valutazione scolastica errata dell'alunno, a causa dell'incompletezza delle informazioni a disposizione del valutatore.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Misure di backup e controllo degli accessi logici. Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti. Tutte le misure esistenti o pianificate individuate.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Limitate	Accettabile
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Molto basso	Adeguate (0,25)	Molto basso

DIFFUSIONE NON AUTORIZZATA DI DATI

RISCHIO		
Diffusione non autorizzata di dati		
POTENZIALE IMPATTO		
Diffusione di informazioni anche sensibili con potenziale impatto sulla dignità e libertà degli interessati. Data Breach. Diffusione di dati personali di minori, diffusione di dati concernenti l'orientamento politico, la razza o la condizione sanitaria degli interessati. Pubblicazione su piattaforme social di dati personali, scarsa sensibilità degli studenti alla privacy dei compagni, Episodi di Cyberbullismo, Negazione del diritto all'oblio.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Misure di backup e controllo degli accessi logici. Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti. Formazione sul tema della cyberbullismo e cybersecurity Tutte le misure esistenti o pianificate individuate.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Limitate	Accettabile
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Molto basso	Adeguate (0,25)	Molto basso

RISCHIO		
Accesso non autorizzato alle sessioni in conference call		
POTENZIALE IMPATTO		
Lezioni disturbate dai troll. Visualizzazione o condivisione di materiale pornografico in conference. Interruzione della lezione.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Gestione sistemi di autorizzazione Controllo degli accessi logici Monitoraggio della piattaforma da parte dei tecnici e degli insegnanti. Formazione sul tema del cyberbullismo e della cybersecurity. Precise disposizioni e prescrizioni sulle modalità di condivisione delle sessioni. Regola dell'intruso: in presenza di soggetti non autorizzati la sessione è immediatamente interrotta e rifissata. Tutte le misure esistenti o pianificate individuate.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Improbabile	Limitate	Accettabile
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Molto basso	Adeguate (0,25)	Molto basso

RISCHIO		
Profilazione degli utenti da parte del gestore della piattaforma		
POTENZIALE IMPATTO		
Gli utenti potrebbero essere profilati anche se minori di anni 13 (COPPA) o senza specifica autorizzazione dei genitori.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Clausole contrattuali con il fornitore dei servizi. Purtroppo, non esistono vere e proprie contromisure.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Marginali	Medio-basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Rilevante	Adeguate (0,5)	Rilevante

RISCHIO		
Lock-in e fidelizzazione degli utenti		
POTENZIALE IMPATTO		
La scuola funge da promotore di servizi a pagamento. Purtroppo, non esistono vere e proprie contromisure.		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Formazione utenti sui rischi legati all'utilizzo di prodotti "gratuiti". Richiesta di specifico consenso/autorizzazione.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Gravi	Rilevante
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Alto	Adeguate (0,25)	Rilevante

RISCHIO		
Utilizzo dell'account della piattaforma per il tracciamento da parte dei motori in attività extra scolastiche		
POTENZIALE IMPATTO		
Una volta loggati in piattaforma, tutte le attività svolte anche successivamente sono tracciate e ricondotte al soggetto in fase di profilazione. Purtroppo, non esistono vere e proprie contromisure		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
Sono fornite specifiche indicazioni sulla necessità di effettuare il log out dalla piattaforma. Purtroppo, non esistono vere e proprie contromisure.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Marginali	Medio-basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Rilevante	Parzialmente Adeguate (0,5)	Rilevante

RISCHIO
Esportazione dati in paesi extra UE con norme e sensibilità non allineate ai principi del GDPR
POTENZIALE IMPATTO
Utilizzi indebiti dei dati. La sentenza del 16 luglio 2020, emessa dalla Corte di giustizia dell'Unione europea (di seguito "CGUE" o "Corte"), ha dichiarato invalida la decisione 2016/1250 della Commissione europea sull'adeguatezza della protezione offerta dal regime dello scudo UE-USA per la protezione dei dati personali, il cosiddetto "Privacy Shield". La CGUE ha ritenuto che i requisiti del diritto interno degli Stati Uniti, e in particolare taluni programmi di sorveglianza che consentono alle autorità pubbliche statunitensi di accedere ai dati personali trasferiti dall'UE agli Stati Uniti per motivi di sicurezza nazionale, non prevedono limitazioni al potere conferito alle autorità statunitensi, né garanzie per soggetti non statunitensi potenzialmente sottoposti a tale sorveglianza. Ne risultano limitazioni alla protezione dei dati personali, che non sono configurate in modo da soddisfare requisiti sostanzialmente equivalenti a quelli previsti dal diritto dell'UE. Tale legislazione non consente ai soggetti interessati diritti azionabili in sede giudiziaria nei confronti delle autorità statunitensi.
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO
Il Garante dello Stato tedesco del Baden-Württemberg ha individuato tra le misure supplementari idonee ad assicurare un livello di protezione adeguato dei dati personali: - i sistemi di crittografia in cui solo l'esportatore possiede la chiave di decriptazione; - i sistemi di anonimizzazione; - i sistemi di pseudonimizzazione, in base a cui l'esportatore può ricollegare i dati ad una determinata persona fisica. Informativa completa, Clausole contrattuali standard ("SCC") Purtroppo, non esistono vere e proprie contromisure. È necessario iniziare a pensare a sistemi alternativi con funzionalità similari.

VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Marginali	Medio-basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Rilevante	Parzialmente Adeguate (0,5)	Rilevante

RISCHIO		
Retention non definita e non legata con la semplice cancellazione dei dati da parte degli utenti		
POTENZIALE IMPATTO		
Riutilizzi indebiti dei dati . Purtroppo, non esistono vere e proprie contromisure		
CONTROMISURE ADOTTATE PER LA MITIGAZIONE DEL RISCHIO		
È necessario iniziare a pensare a sistemi alternativi con funzionalità similari. Purtroppo, non esistono vere e proprie contromisure. Clausole contrattuali con il fornitore.		
VALUTAZIONE RISCHIO INTRINSECO		
Probabilità	**Conseguenza**	**Rischio intrinseco - Ri**
Probabile	Marginali	Medio-basso
VALUTAZIONE RISCHIO NORMALIZZATO *Viene preso in considerazione il livello di adeguatezza peggiore rispetto alle misure di sicurezza attuate per il pericolo ed i rispettivi rischi*		
Rischio intrinseco - Ri	**Adeguatezza Misure** (indice **Vulnerabilità – Vu)**	**Rischio normalizzato - RN**
Rilevante	Parzialmente Adeguate (0,5)	Rilevante