

Titolare del Trattamento



www.liceocampanellalamezia.edu.it

**LICEO STATALE  
Tommaso  
Campanella**  
LAMEZIA TERME

**Liceo Statale “Tommaso Campanella”**  
*Liceo Linguistico – Liceo delle Scienze Umane – Liceo Economico-Sociale – Liceo Musicale-Coreutico*  
via Bachelet – 88046 LAMEZIA TERME (CZ)  
Cod. Meccanografico: CZPM03000C – Cod. Fiscale: 82006590796  
☎ 0968.22047 – ✉ [CZPM03000C@istruzione.it](mailto:CZPM03000C@istruzione.it)

## **VALUTAZIONE D’IMPATTO SULLA PROTEZIONE DEI DATI (DPIA\*) PER L’UTILIZZO DI PIATTAFORME CLOUD AI FINI DELLO SVOLGIMENTO DI ATTIVITA’ DI DDI E AMMINISTRATIVE**

**Responsabile della Valutazione: Susanna Mustari**

**Posizione:** Dirigente Scolastico

*\*DPIA realizzata in parte sulla base del modello messo a disposizione dalla CNIL (Autorità francese per la protezione dei dati) e tradotta in italiano con la collaborazione del Garante per la protezione dei dati.*

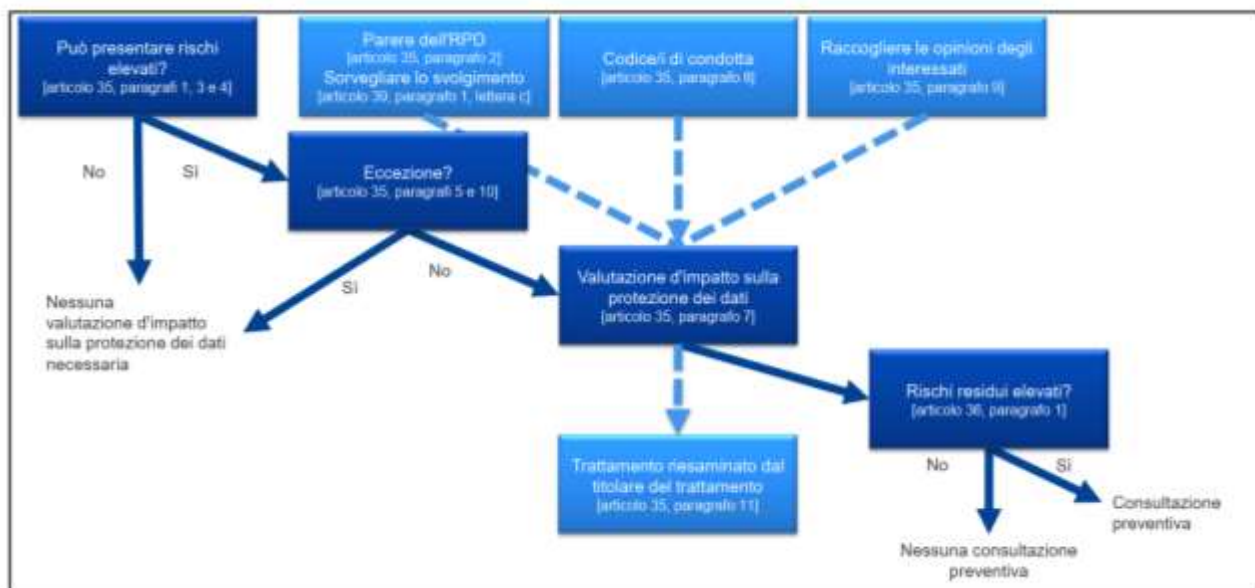
### **Oggetto della DPIA**

Piattaforma cloud Google Workspace.

### **Introduzione e motivi della DPIA**

La DPIA (Data Protection Impact Assessment), è una valutazione preliminare eseguita dal titolare del trattamento dei dati personali, relativa agli impatti e ai rischi determinati da un determinato trattamento dati.

Secondo il GDPR, non è necessario/obbligatorio svolgere una valutazione d'impatto per ciascun trattamento, ma solo per quelli che "possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (art. 35 Regolamento UE 2016/679).



I criteri da prendere in considerazione per l'obbligo della DPIA (secondo il Gruppo art.29 "Comitato Europeo della protezione dei dati") sono i seguenti:

- Profilazione
- Decisioni automatizzate che producono significativi effetti giuridici
- Monitoraggio sistematico
- Trattamenti di dati sensibili, giudiziari o di natura estremamente personale
- Trattamenti di dati personali su larga scala
- Dati relativi a soggetti vulnerabili
- Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative
- Trattamenti che, di per sé, potrebbero impedire agli interessati di esercitare un diritto

In presenza di almeno due di questi criteri, la DPIA è necessaria.

In relazione alla specifica piattaforma oggetto della valutazione, la sua iniziale adozione a seguito dei Decreti relativi alla gestione della pandemia da Covid-19 che prevedevano la continuità didattica tramite DAD (Didattica a Distanza), non prevedeva DPIA. La scelta dello strumento fu fatta sulla base delle piattaforme in quel momento immediatamente disponibili, suggerite dal Ministero dell'Istruzione tramite un elenco di soluzioni messo a disposizione, e con il requisito della certificazione Agid. In quel contesto, lo stesso Garante privacy ha emesso il provvedimento n.64 del 26 marzo 2020 "Didattica a distanza: prime indicazioni", nel quale indicava come non necessaria la DPIA e specificava che "L'Autorità vigilerà sull'operato dei fornitori delle principali piattaforme per la didattica a distanza, per assicurare che i dati di docenti, studenti e loro familiari siano trattati nel pieno rispetto della disciplina di protezione dati e delle indicazioni fornite dalle istituzioni scolastiche e universitarie".

Con l'intervento della sentenza Schrems-II che ha invalidato il Privacy Shield (Scudo privacy) e reso non conforme il trasferimento dati negli USA, il Titolare ha limitato l'utilizzo della piattaforma in attesa di chiarimenti da parte del Garante e/o del nuovo accordo UE/USA. In assenza di entrambi, e in considerazione delle attività didattiche e operative della scuola, si è riscontrata la necessità di riprendere l'utilizzo della piattaforma, per consentire il corretto svolgimento delle attività di DDI oltre all'attuazione degli obiettivi stabiliti dal Piano Nazionale Scuola Digitale nell'ambito del PNRR.

## Processo di valutazione

Il processo che porta alla valutazione del rischio prevede alcune fasi, così riassunte:

### Fase 1: identificazione dei trattamenti

Consiste nell'individuare tutti gli elementi del trattamento dati:

- Tipologia di dati
- Finalità

- Categorie di interessati
- Modalità di trattamento
- Misure tecniche/organizzative
- Destinatari
- Eventuale trasferimento extra UE (nel caso è necessario effettuare anche la TIA)

### **Fase 2: Panoramica dei rischi**

Vengono individuati i potenziali rischi, cioè la probabilità con cui un evento dannoso possa verificarsi, e le relative conseguenze, determinando una scala di probabilità del rischio che va da “improbabile” a “quasi certo” e una scala di incidenza delle conseguenze che va da “trascurabili” a “gravissime”.

### **Fase 3: Valutazione del rischio ed eventuali misure correttive**

Si valutano rischi e conseguenze, determinando l’esito della DPIA.

## **Informazioni preliminari**

---

**Parere degli interessati:** non è stato chiesto il parere agli interessati. Il Titolare del trattamento, nel rispetto del principio di accountability, definisce gli strumenti del trattamento dati funzionali al perseguimento di finalità istituzionali connesse all’esecuzione di un compito di interesse pubblico o connesso all’esercizio di pubblici poteri. Gli interessati sono adeguatamente informati su tutti gli aspetti del trattamento e possono, oltre ad esercitare i propri diritti, partecipare al miglioramento e adeguamento del trattamento qualora dovessero riscontrare criticità o volessero suggerire miglioramenti.

**Categorie di interessati:** personale scolastico, alunni, familiari/tutori alunni

## **Contesto**

---

### **Panoramica**

#### **Qual è il trattamento in considerazione?**

Il trattamento riguarda l’utilizzo delle nuove tecnologie, nello specifico l’utilizzo della piattaforma cloud per lo svolgimento di attività connesse alla DDI e la fruizione di documenti digitali, l’attuazione di un’ ampliata e rinnovata offerta formativa che prevede l’utilizzo di strumenti digitali e forme nuove di apprendimento, l’organizzazione della didattica, le funzioni amministrative connesse, le attività di coordinamento/organizzazione/svolgimento degli OOC da remoto.

L’utilizzo della piattaforma può avvenire, da parte del personale e degli alunni, sia a scuola durante le ore di attività, sia in ambito domestico, con strumenti messi a disposizione dal titolare del trattamento (pc, tablet) o tramite strumenti propri dell’interessato (pc, tablet, smartphone).

L’interessato può utilizzare la connessione internet della scuola (se messa a disposizione) oppure il proprio piano dati internet utilizzato sul proprio dispositivo.

#### **Quali sono le responsabilità connesse al trattamento?**

I soggetti coinvolti nel trattamento dati sono diversi, con funzioni complementari e con il compito di cooperare per una corretta gestione della piattaforma e del relativo trattamento dati. Vediamo quali sono le principali figura individuabili:

- **Il Titolare del trattamento**, è la persona fisica o giuridica, l’autorità pubblica [...] che determina le finalità e i mezzi del trattamento di dati personali (art. 4 GDPR). In questo caso è l’Amministrazione scolastica legalmente rappresentata dal Dirigente scolastico, che determina quali dati trattare, per quali finalità, con quali strumenti, con quali modalità.
- **I docenti**, svolgono il ruolo di Incaricati al trattamento e agiscono sotto l’autorità del titolare del trattamento. Producono documenti didattici e contenuti che condividono con gli alunni della classe e gruppi di lavoro, su cui devono avere supervisione per assicurarsi che tutti gli alunni agiscano nel rispetto delle regole e delle prescrizioni di utilizzo fornite.
- **L’amministratore della piattaforma (admin)**, è il soggetto che accede alla consolle e ha i privilegi necessari per gestire i servizi e gli utenti.
- **Il Responsabile del trattamento**, è il soggetto che tratta in modo stabile e continuativo i dati per conto del titolare, per effetto di un contratto o atto giuridico che vincoli il responsabile al titolare. Deve

presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del GDPR e garantisca la tutela dei diritti dell'interessato. In questo caso, il Responsabile del trattamento è Google LLC.

- **L'amministratore di sistema**, è nominato dal DS ed ha il compito di verificare la sicurezza informatica delle risorse hardware, provvedendo ad attivare le misure necessarie quali antivirus, anti malware, firewall, impostazioni di accesso fisico.

### **Ci sono standard applicabili al trattamento?**

La scelta della piattaforma è stata effettuata, oltre che sulla base delle indicazioni date dal MI nel 2020, soprattutto tenendo in considerazione le disposizioni Agid, che prevedono che le PA utilizzino servizi cloud abilitati da Agid (oggi ACN). La scuola si è dotata, inoltre, di un regolamento sulla DDI redatto sulla base delle indicazioni del MI "Linee guida per la Didattica Digitale Integrata (DDI)" e sulla base delle indicazioni del Garante privacy "Didattica a distanza: prime indicazioni" di marzo 2020. Sono inoltre periodicamente consultate le raccomandazioni adottate dall'Edpb (Garante Privacy Europeo) sui requisiti dei servizi cloud adottati dalle PA. Non sono stati identificati, al momento, codici di condotta, standard o certificazioni applicabili.

## **Dati, processi e risorse di supporto**

### **Quali sono i dati trattati?**

I dati trattati tramite la piattaforma sono quelli relativi e necessari allo svolgimento di attività digitali, sia di natura strettamente didattica che di natura amministrativa/organizzativa. Sulla piattaforma vengono condivisi materiali didattici predisposti dai docenti e/o dagli alunni, documenti organizzativi come le programmazioni, gli orari, i libri di testo, i calendari degli incontri e in generale i documenti la cui condivisione tra docenti è funzionale al corretto e funzionale svolgimento dei compiti di loro pertinenza. I dati trattati sono minimizzati a quelli strettamente necessari, ma l'utilizzo di un account personale nella forma nome.cognome@sitoscuola.edu.it determina il trattamento in chiaro del nome utente, per poter essere correttamente ed univocamente identificato all'interno della piattaforma. Le disposizioni sull'utilizzo della piattaforma cloud prevedono di non trattare tramite la stessa nessuna categoria particolare di dati (ex sensibili) né di condividere documenti che possano ricondurre a dati di tale natura.

### **Qual è il ciclo di vita del trattamento dei dati (descrizione funzionale)?**

L'utilizzo della piattaforma è subordinato alla creazione e assegnazione di un account personale ad ogni interessato. Nel rapporto docenti/alunni, i docenti condividono i documenti didattici nelle classi virtuali rendendoli disponibili agli alunni, che potranno solo acquisire i documenti oppure rielaborare gli stessi in quanto prova/compito di classe, in base alle disposizioni del docente. Gli elaborati condivisi dall'alunno saranno poi acquisiti dal docente, che procederà all'archiviazione quando la prova didattica sarà ritenuta conclusa. Nelle attività di natura organizzativa/amministrativa, sulla piattaforma sono predisposti ambienti di comunicazione e condivisione per il personale, in cui vengono condivise informazioni e documenti funzionali all'organizzazione delle attività e all'espletamento delle procedure previste (programmazioni, orari, calendari, ecc...).

### **Quali sono le risorse di supporto ai dati?**

La piattaforma cloud prevede diversi servizi per la gestione della DDI e la condivisione di documenti (come Gmail, Calendar, Classroom, Drive) raggiungibili attraverso strumenti digitali (pc, tablet, smartphone) e una connessione internet. Tali strumenti sono adeguatamente impostati tramite le funzionalità messe a disposizione all'amministratore della piattaforma, determinando le regole di condivisione ed escludendo i servizi aggiuntivi che non siano strettamente necessari. L'utilizzo di strumenti di comunicazione (es. email) è circoscritto a comunicazioni di natura personale/individuale, veicolando comunicazioni e informazioni di natura collettiva attraverso altri strumenti (es. Registro elettronico), in modo da limitare le informazioni veicolate tramite la piattaforma cloud. Vengono condivisi file didattici, presentazioni, altri materiali tramite le classi virtuali e altri ambienti di condivisione come Drive, mentre la condivisione di calendari (OOCC, incontri scuola-famiglia, altri eventi) avviene tramite la funzione specifica.

## Principi fondamentali

---

### **Proporzionalità e necessità**

#### **Gli scopi del trattamento sono specifici, espliciti e legittimi?**

Gli scopi del trattamento sono quelli di perseguire le finalità istituzionali del titolare del trattamento, come attuare il Piano Triennale dell'Offerta Formativa, che prevede nuove metodologie di apprendimento e strumenti di DDI. Inoltre, il CAD prevede la transizione digitale delle PA per efficientare i servizi mentre il passaggio al cloud è uno dei principali obiettivi del Piano Nazionale Scuola Digitale nell'ambito delle misure del PNRR, di cui la scuola è beneficiaria. L'obiettivo è dunque quello di formare gli alunni ad un consapevole e funzionale uso delle tecnologie digitali, per poter guidare i più piccoli e preparare i più grandi verso un percorso di studi universitari e/o un mondo del lavoro che richiede competenze e capacità digitali. Del trattamento sono esplicitamente informati gli interessati con specifica informativa, che definisce tutti gli aspetti del trattamento e la legittimità dello stesso da parte del titolare, il quale agisce per il perseguimento di finalità istituzionali connesse all'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nell'ambito di tali finalità, il titolare definisce quali dati trattare e con quali strumenti, e questa DPIA è volta a valutare proprio il rischio di tale scelta.

#### **Quali sono le basi legali che rendono lecito il trattamento?**

L'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri. Nello specifico, la scuola organizza la propria attività per lo svolgimento, primariamente, degli obiettivi prefissati nel PTOF (Piano Triennale dell'Offerta Formativa), che rappresenta il documento identificativo della scuola e contiene un'indicazione chiara e dettagliata di obiettivi, linea d'azione e mezzi a disposizione per raggiungerli. Agisce poi in conformità del CAD (Codice dell'Amministrazione Digitale), il quale prevede e promuove l'uso delle nuove tecnologie nella PA per le attività amministrative e organizzative.

#### **I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?**

I dati trattati tramite l'utilizzo della piattaforma cloud sono dati personali (es. nominativo, indirizzo IP del dispositivo) e informazioni didattiche (es. lezioni, programmazioni). I dati trattati, seppur limitati più possibile rispetto alle finalità, consentono di identificare l'utente in considerazione del nominativo inserito nell'account individuale, assegnato ad ogni interessato per poter identificare in maniera univoca l'utente all'interno della piattaforma. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.

#### **I dati sono esatti e aggiornati?**

I dati vengono verificati e aggiornati periodicamente, eliminando gli utenti non più operativi, archiviando/cancellando i file non più pertinenti. Eventuali segnalazioni di rettifica da parte degli interessati vengono prese in carico dall'amministratore della piattaforma, dopo averne verificato l'attendibilità e applicabilità.

#### **Qual è il periodo di conservazione dei dati?**

La conservazione dei dati è effettuata per il periodo necessario al perseguimento delle finalità. Successivamente, per i documenti rilevanti ai fini didattici/amministrativi, si procede all'archiviazione dei dati per il tempo previsto dalla normativa di riferimento. Per i documenti che costituiscono prove di valutazione, ad esempio, l'archiviazione ha la durata di almeno un anno e comunque deve rispettare i tempi previsti dalla circolare n.44 del 2005 della Direzione Generale degli Archivi. Altri tipi di prove e documenti, possono essere archiviati fino alla fine dell'anno scolastico o del percorso in cui si inserisce il documento.

### **Misure a tutela dei diritti degli interessati**

#### **Come sono informati del trattamento gli interessati?**

Gli interessati sono informati del trattamento dati con specifica e dettagliata informativa (art. 13 GDPR), contenente i dettagli e le caratteristiche del trattamento, anche e soprattutto in riferimento al trasferimento

dati extra UE. L'Informativa è pubblicata sul sito web del titolare del trattamento e notificata a tutti gli interessati tramite il canale di comunicazioni del Registro elettronico.

### **Come fanno gli interessati ad esercitare i propri diritti?**

Gli interessati possono esercitare i propri diritti contattando gli uffici del titolare del trattamento, chiedendo informazioni sui propri dati o l'esercizio di un diritto di cui dagli artt. 15 a 23 del GSPR, nella misura in cui applicabili alla tipologia di trattamento.

### **Gli obblighi dei Responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?**

In base all'Emendamento sul trattamento dei dati (EDT) di Google Workspace, Google svolge il ruolo di Responsabile del trattamento dei dati personali dei clienti che vengono trasmessi, archiviati, inviati o ricevuti dal titolare attraverso i servizi di Google Workspace e tratta tali dati per suo conto e dietro sue istruzioni. I trattamenti operati da Google LLC sono inoltre regolamentati tramite Cloud Data Processum Addendum (CDPA), dove sono specificati gli obblighi in carico al Responsabile del trattamento. Il Contratto prevede che il Cliente è il titolare del trattamento e Google è il Responsabile del trattamento. Ai sensi del Contratto, il Cliente sarà tenuto ad adempiere ai propri obblighi di Titolare del trattamento e Google sarà tenuto ad adempiere ai propri obblighi di Responsabile del trattamento. Tuttavia, è opportuno sottolineare che questo Titolare del trattamento (la scuola), nella definizione di clausole contrattuali ha bassissimo se non nullo potere contrattuale, per cui è impossibile per lo stesso ottenere garanzie rafforzate e più tutelanti, ad esempio, in relazione al trasferimento dati extra UE. Il fornitore Google LLC è inserito, inoltre, nell'elenco SaaS (Software as a Service) della Agenzia per la Cybersicurezza Nazionale (ex Agid), e in base a ciò è stata fatta una valutazione in merito ai requisiti di sicurezza e affidabilità informatica della piattaforma.

### **In caso di trasferimento dati al di fuori dell'Unione Europea, i dati godono di una protezione equivalente?**

No. I dati trattati sono soggetti a trasferimento dati extra UE verso gli USA. A seguito della sentenza Schrems-II, che ha invalidato il Privacy Shield, manca una dichiarazione di adeguatezza del trasferimento e la normativa statunitense sul trattamento dati non è conforme al GDPR. Per questo motivo, si rende necessaria l'effettuazione del TIA (Valutazione d'impatto dei trasferimenti dati extra UE).

## **Rischi**

Come abbiamo visto all'inizio di questa DPIA, alla Fase 1 "Identificazione dei trattamenti", seguono la Fase 2 "Panoramica dei rischi" e la Fase 3 "Valutazione del rischio ed eventuali misure correttive".

Il livello del rischio può essere misurato numericamente utilizzando due valori:

- 1) Probabilità di accadimento (P)
- 2) Conseguenze (C)

Il Livello di Rischio (LR) è dato dunque dalla relazione:  $LR=P \times C$

Alla probabilità P e alle conseguenze C sono associati valori numerico in relazione alla loro incidenza:

<b>P</b>	<b>Probabilità di accadimento</b>	<b>C</b>	<b>Conseguenze</b>
1	Improbabile	1	Trascurabili
2	Poco probabile	2	Limitate
3	Probabile	3	Gravi
4	Certo	4	Gravissime

Il livello di rischio LR, dunque, potrà variare da un valore minimo 1 a un valore massimo 16, così valutabile:

<b>Entità del rischio</b>	<b>Valori di riferimento</b>
Poco rilevante	$1 \geq LR \leq 3$
Basso	$4 \geq LR \leq 7$
Alto	$8 \geq LR \leq 12$
Altissimo	$13 \geq LR \leq 16$

Così è possibile ricavare, per ogni attività di trattamento, il Livello di Rischio di potenziale accesso illegittimo, modifica, perdita, distruzione di dati non autorizzata.

I livelli P e C vengono chiaramente stimati e assegnati ai rischi dal titolare in relazione ad una valutazione generale dei propri trattamenti, alla luce di tutti i parametri specificati nel corso di questa DPIA.

## **Misure esistenti o pianificate**

### **Controllo degli accessi**

Gli accessi logici degli utenti avvengono attraverso l'account individuale assegnato ad ognuno ed autorizzato, con eventuali limitazioni in base alla tipologia di utente (docente, alunno). Gli account di utenti non più interessati del titolare (es. docenti non più in servizio o alunni che si trasferiscono) vengono disattivati.

### **Minimizzare la quantità di dati personali**

I dati personali vengono minimizzati più possibile, compatibilmente con il perseguimento delle finalità e il raggiungimento degli obiettivi. Tuttavia, consentono di identificare l'utente in considerazione del nominativo inserito nell'account individuale, assegnato ad ogni interessato per poter identificare in maniera univoca l'utente all'interno della piattaforma. Vengono inoltre acquisite dalla piattaforma una serie di altre informazioni, come ID del dispositivo, browser, sistema operativo, lingua selezionata, in parte classificabili come dati personali. Non vengono gestiti dati sensibili né documenti che possano ricondurre a tale categoria di dati.

### **Anonimizzazione dei dati**

L'account contiene in chiaro il nome dell'utente, per poter identificare in maniera univoca il soggetto all'interno della piattaforma. La gestione di account anonimi non sarebbe attuabile, perché non consentirebbe di effettuare sulla piattaforma il controllo degli accessi logici compromettendo la sicurezza della stessa. Vengono anonimizzati/pseudonimizzati i dati eventualmente contenuti in documenti condivisi, la cui natura non consente di indicare le informazioni in chiaro (circostanza rara e non prevista per il trattamento dati tramite la piattaforma). Il fornitore/responsabile cripta inoltre i dati per impostazione predefinita.

### **Misure di sicurezza informatica**

I sistemi di sicurezza dei dispositivi in uso presso e della scuola vengono periodicamente verificati e aggiornati e sono dotati di antivirus, anti malware e firewall. I pc amministrativi sono dotati di credenziali per l'accesso, mentre quelli dei laboratori ne sono sprovvisti per motivi ovvi (utilizzo trasversale da parte di tutti gli alunni), i quali tuttavia non contengono alcun tipo di documenti e informazioni, ma vengono solo utilizzati per attività didattiche ed esercitazioni. Le misure di sicurezza proprie della piattaforma sono attuate direttamente dal fornitore/responsabile del servizio (Google LLC).

### **Istruzioni agli operatori**

Gli operatori sono stati istruiti sul corretto uso della piattaforma, attraverso attività formative e informative, specifici regolamenti e netiquette rivolte a personale e alunni. Sono state fornite informazioni e indicazioni sia da un punto di tecnico, per il corretto uso dello strumento e delle funzioni messe a disposizione, sia da un punto di vista del trattamento dati, per un adeguato uso dei dati e dei documenti da poter condividere tramite la piattaforma e una corretta valutazione dei dati da escludere da questo tipo di trattamento. Le istruzioni e netiquette sono state fornite anche sull'uso della videoconferenza (in passato utilizzata anche per la DAD, ora solo per gli OOC, le riunioni di gruppi, il coordinamento).

## **Accesso illegittimo ai dati**

### **Fonti del rischio**

Il rischio di un accesso illegittimo ai dati può avvenire per cause dolose o colpose/accidentali:

- Cessione a terzi non autorizzati delle proprie credenziali di accesso
- Errato invio di documenti a soggetti terzi diversi dal destinatario
- Errata attribuzione dei permessi sulla piattaforma

- Azione dolosa di hackeraggio sulla piattaforma da parte di terzi
- Condivisione di documenti non idonei (es. con dati sensibili o informazioni strettamente personali) sulla piattaforma o invio non autorizzato tramite email

### **Misure per mitigare il rischio**

Le misure tecniche e organizzative utili a mitigare il rischio di un accesso illegittimo sono quelle descritte nel corso di questa DPIA, e cioè (elenco in continuo aggiornamento):

- Impostazioni tecniche sulla piattaforma
- Formazione tecnica agli utenti
- Definizione delle policy sul trattamento dati
- Verifica periodi degli utenti attivi e di quelli da disattivare
- Controllo degli accessi logici
- Minimizzazione dei dati
- Criptazione per impostazione predefinita
- Anonimizzazione e pseudonimizzazione quando possibile e/o necessario
- Periodici appelli per una corretta gestione delle credenziali di accesso
- Archiviazione/Razionalizzazione dei documenti e Backup
- Sistema firewall

### **Stima della probabilità e della gravità del rischio**

Sulla base delle misure adottate (che vengono costantemente monitorate e implementate se necessario), delle indicazioni agli utenti sulla corretta gestione della piattaforma (i quali vengono periodicamente sollecitati ad agire in modo attento e nel rispetto della sicurezza), la probabilità che il rischio si possa verificare (**P**) è stimata come *Poco probabile* (P=2).

In base alla natura dei dati trattati (considerando che non è previsto il trattamento di dati sensibili), possiamo valutare le conseguenze (**C**) di un eventuale accesso illegittimo ai dati come *Limitate* (C=2).

### **Stima del Livello di Rischio LR**

Sulla base dei parametri sopra valutati P=2 e C=2, il livello di rischio di un Accesso illegittimo ai dati è pari a  $LR=P \times C \rightarrow LR=2 \times 2=4$  (in una scala che va da 1 a 16)

## **Modifiche indesiderate ai dati**

### **Fonti del rischio**

Il rischio di una modifica indesiderata ai dati può avvenire per cause dolose o colpose/accidentali:

- Errore umano (ad es. modifiche di dati errati nel giusto documento o modifica di dati esatti nel documento sbagliato)
- Volontà/dolo di un utente abilitato di modificare dati per i quali non si è autorizzato ad agire
- Volontà/dolo di un soggetto esterno che riesce ad accedere alla piattaforma e a modificare i dati

### **Misure per mitigare il rischio**

Le misure tecniche e organizzative utili a mitigare il rischio di un accesso illegittimo sono quelle descritte nel corso di questa DPIA, e cioè (elenco in continuo aggiornamento):

- Impostazioni tecniche sulla piattaforma
- Formazione tecnica agli utenti
- Definizione delle policy sul trattamento dati
- Verifica periodi degli utenti attivi e di quelli da disattivare
- Controllo degli accessi logici
- Periodici appelli per una corretta gestione delle credenziali di accesso
- Archiviazione/Razionalizzazione dei documenti e Backup

### **Stima della probabilità e della gravità del rischio**

Sulla base delle misure adottate (che vengono costantemente monitorate e implementate se necessario), delle indicazioni agli utenti sulla corretta gestione della piattaforma (i quali vengono periodicamente sollecitati ad agire in modo attento e nel rispetto della sicurezza), la probabilità che il rischio si possa verificare (**P**) è stimata come *Improbabile* (P=1).



In base alla natura dei dati trattati (considerando che non è previsto il trattamento di dati sensibili), e che tramite le operazioni di archiviazione e backup è possibile recuperare i dati esatti, possiamo valutare le conseguenze (C) di un eventuale modifica indesiderata ai dati come *Limitate* (C=2).

#### Stima del Livello di Rischio LR

Sulla base dei parametri sopra valutati P=1 e C=2, il livello di rischio di una Modifica indesiderata ai dati è pari a  $LR=P \times C \rightarrow LR=1 \times 2=3$  (in una scala che va da 1 a 16)

### Perdita di dati

#### Fonti del rischio

Il rischio di una perdita dati può avvenire per cause dolose o colpose/accidentali:

- Errore umano (ad es. cancellazione di dati all'interno di un documento e/o eliminazione di un intero file)
- Volontà/dolo di un utente abilitato di cancellare dei dati per i quali non si è autorizzato ad agire
- Volontà/dolo di un soggetto esterno che riesce ad accedere alla piattaforma e a cancellare i dati
- Problemi tecnici (hardware o software) che possono determinare un'accidentale perdita di dati

#### Misure per mitigare il rischio

Le misure tecniche e organizzative utili a mitigare il rischio di una perdita dati sono quelle descritte nel corso di questa DPIA, e cioè (elenco in continuo aggiornamento):

- Impostazioni tecniche sulla piattaforma
- Formazione tecnica agli utenti
- Definizione delle policy sul trattamento dati
- Verifica periodi degli utenti attivi e di quelli da disattivare
- Controllo degli accessi logici
- Periodici appelli per una corretta gestione delle credenziali di accesso
- Archiviazione/Razionalizzazione dei documenti e Backup
- Sistemi anti malware e firewall

#### Stima della probabilità e della gravità del rischio

Sulla base delle misure adottate (che vengono costantemente monitorate e implementate se necessario), delle indicazioni agli utenti sulla corretta gestione della piattaforma (i quali vengono periodicamente sollecitati ad agire in modo attento e nel rispetto della sicurezza), la probabilità che il rischio si possa verificare (P) è stimata come *Poco probabile* (P=2).

In base alla natura dei dati trattati (considerando che non è previsto il trattamento di dati sensibili), e che tramite le operazioni di archiviazione e backup è possibile recuperare i dati all'ultima versione disponibile, possiamo valutare le conseguenze (C) di un eventuale perdita di dati come *Limitate* (C=2).

#### Stima del Livello di Rischio LR

Sulla base dei parametri sopra valutati P=1 e C=2, il livello di rischio di una perdita di dati è pari a  $LR=P \times C \rightarrow LR=2 \times 2=4$  (in una scala che va da 1 a 16)

#### Livello di Rischio (LR)

Rischio	Probabilità (P)	Conseguenze (C)	Livello di Rischio (LR)
Accesso illegittimo	2	2	4
Modifiche indesiderate	1	2	3
Perdita	2	2	4

Alla luce delle misure adottate e della tipologia di dati trattati, delle valutazioni circa probabilità e conseguenze del verificarsi di un evento di rischio a cui sono stati attribuiti dei valori ritenuti adeguati rispetto al quadro generale, si evidenzia come i Livelli di Rischio (LR) siano del tutto accettabili e molto al di sotto della soglia massima ritenuta accettabile.

## VALUTAZIONE D'IMPATTO DEI TRASFERIMENTI DATI EXTRA UE (TIA\*)

*Per la valutazione dei rischi connessi al trasferimento dati extra Ue (in particolare verso gli USA) ai sensi del Regolamento Generale sulla Protezione dei Dati dell'UE (GDPR) e delle clausole contrattuali standard dell'UE (UE SCC)*

*\*TIA redatta sulla base del modello messo a disposizione della IAPP (International Association of Privacy Professionals). Autore originario: David Rosenthal (original version at [www.rosenthal.ch](http://www.rosenthal.ch))\* (Licensing: See bottom).*

\* La presente TIA è stata predisposta su un separato documento in formato excel, le cui tabelle sono inserite all'interno della presente valutazione complessiva per riunire in un unico documento il complesso delle analisi effettuate.

## **Introduzione**

Nella DPIA è emerso che la piattaforma cloud utilizzata, Google Workspace, effettua trasferimento dati extra UE verso gli USA, per cui questo tipo di trattamento necessita della TIA, che è un'ulteriore valutazione del rischio, un'analisi del livello di sicurezza del rispettivo paese terzo verso il quale i dati devono essere trasferiti. Ci sono un esportatore (titolare del trattamento/scuola), un importatore (fornitore/Google) e un Paese terzo di destinazione (USA).

Nella redazione della TIA sono stati definiti una percentuale massima di accesso ritenuta accettabile e un arco temporale di lungo termine, per calcolare la probabilità di accesso annuale da parte del Paese terzo. Ritenuta accettabile una probabilità del 50% che un accesso avvenga ogni 40 anni, la relativa probabilità di accesso annuale è pari all'1,53% (come specificato nel successivo punto 2 delle tabelle).

Google mette a disposizione (nel Transparency Report) le statistiche e le richieste di accesso da parte dei Governi, e a livello mondiale tale probabilità di accesso è pari a circa lo 0,03%, decisamente più basso del valore considerato accettabile e calcolato nella misura dell'1,53%.

Segue il dettaglio della Valutazione effettuata, che si sviluppa in 5 punti:

Punto 1: Descrizione del trasferimento previsto

Punto 2: Definizione dei parametri TIA

Punto 3: Definizione delle misure attuate

Punto 4: Valutare il rischio di accesso legale nella giurisdizione di destinazione

Punto 5: Conclusioni

Punto 1: descrizione del trasferimento previsto		
a)	Esportatore dei dati:	Titolare del Trattamento
b)	Paese dell'esportatore dei dati:	Italia
c)	Importatore di dati:	Google LLC
d)	Paese dell'importatore dei dati:	USA
e)	Contesto e finalità del trasferimento dati:	Utilizzo della piattaforma Google Workspace for Education, per finalità di Didattica Digitale Integrata, metodologie formative innovative, per organizzazione di eventuali servizi formativi e/o OOC in remoto (in caso di riscontrate esigenze).
f)	Categorie di interessati:	Dipendenti, Alunni, Famiglie/Tutori, Soggetti esterni alla scuola (in caso di corsi di formazione da svolgere online).
g)	Categorie di dati personali soggetti a trasferimento:	Nominativo, indirizzo email, eventuali dati sulla didattica, informazioni sul dispositivo (ad esempio modello di hardware, versione del sistema operativo, identificatori univoci del dispositivo e informazioni relative alla rete mobile, incluso il numero di telefono), informazioni di log, informazioni sugli eventi del dispositivo e indirizzo IP (protocollo Internet) dell'utente, informazioni sulla posizione ricavate tramite varie tecnologie (tra cui l'indirizzo IP, GPS e altri sensori), numeri specifici delle applicazioni (come il numero di versione dell'applicazione), cookie o tecnologie analoghe utilizzate per acquisire e memorizzare le informazioni relative a un browser o dispositivo (come la lingua preferita e altre impostazioni).
h)	Categorie particolari di dati personali (ex sensibili):	Le categorie particolari di dati (ex sensibili) e i dati giudiziari vengono trattati tramite la piattaforma solo se strettamente necessario e minimizzando in relazione alle specifiche finalità, ma in generale queste categorie di dati non necessitano di essere trattati tramite la piattaforma.
i)	Attuazione tecnica del trasferimento:	Tramite le applicazioni e i servizi web dell'importatore Google LLC (in particolare della piattaforma Workspace for Education), che all'atto di sottoscrizione del contratto è nominato Responsabile del Trattamento.
j)	Misure tecniche e organizzative:	Accessi individuali tramite account personale fornito dalla scuola, crittografia in transito e a riposo, attivazione delle misure tecniche messe a disposizione dall'importatore, minimizzazione dei dati trattati, limitazione e inibizione di servizi non necessari rispetto alle finalità, istruzioni e formazione per gli utenti.

Punto 2: definizione dei parametri TIA			Analisi
a)	Anno di inizio del trasferimento:	2023	
b)	Periodo di valutazione in anni:	5	<i>La valutazione sarà nuovamente effettuata alla fine del periodo di validità della presente valutazione.</i>
c)	Determinazione del rischio residuo accettabile di accesso legale all'estero: se la probabilità che un accesso legale a distanza di 40 anni è pari al 50% (soglia massima ritenuta accettabile), allora la probabilità annuale che tale accesso avvenga è così bassa che si ha ragionevole motivo di credere che non si verificherà in tale periodo.	40	<i>Si stabilisce in 40 anni il periodo ritenuto accettabile per il rischio di un potenziale accesso legale da parte delle autorità statunitensi, fissando ad una soglia del 50% la percentuale massima ritenuta accettabile.</i>
	Probabilità calcolata in base a quanto sopra:	1,53%	<i>In base ai parametri di cui sopra, si calcola la probabilità annuale che un accesso all'estero possa avvenire.</i>
d)	Giurisdizione di riferimento per la quale viene effettuata la TIA:	USA	
e)	Leggi USA pertinenti prese in considerazione:	Section 702 FISA, EO 12.333 (and PPD-28)	

**Punto 3: definizione delle misure attuate**

			Analisi
a)	Sarebbe possibile, da un punto di vista pratico, tecnico ed economico, che l'esportatore di dati trasferisse invece i dati personali in questione in un luogo in un paese inserito nella whitelist?	No	<i>I servizi offerti dall'importatore Google LLC (per completezza, sicurezza informatica, economicità, facilità di utilizzo, varietà e tipologia dei servizi) non sono individuabili, in base alle nostre ricerche, in altri fornitori che non effettuano trasferimento dati extra UE.</i>
b)	I dati personali vengono trasferiti in base a una delle deroghe ai sensi dell'articolo 49 del GDPR?	Si	<i>Art. 49, comma 1a: consenso dell'interessato Art. 49, comma 1d: per importanti motivi di interesse pubblico In base al tipo di trattamento e alla tipologia di interessato</i>
c)	I dati personali in questione sono trasmessi alla giurisdizione di destinazione in chiaro (ossia non esiste una crittografia appropriata in transito)?	No	<i>Parte dei dati trasmessi sono crittografati attraverso tecniche attuate dall'importatore (Responsabile del Trattamento), a cui si possono aggiungere chiavi di crittografia esterne lato client.</i>
d)	I dati personali in questione sono accessibili nella giurisdizione di destinazione in chiaro da parte dell'importatore/destinatario dei dati o di terzi (ossia i dati non sono completamente crittografati o è possibile accedere alle chiavi per decrittografare)?	Si	<i>L'accesso legale all'estero è almeno tecnicamente possibile I dati trasferiti sono tecnicamente accessibili e leggibili in chiaro.</i>
e)	I dati personali in questione sono protetti da un meccanismo di trasferimento conforme al GDPR o a clausole contrattuali standard dell'UE (SCC, BCR) approvate, che possa essere rispettato nella misura consentita dalla giurisdizione di destinazione?	Si	<i>Verificare che il meccanismo rimanga in vigore Il trasferimento, in attesa del nuovo accordo UE/USA, è basato sulla nuova SCC approvata dell'UE. Non si ha motivo di credere che l'importatore (Responsabile del Trattamento) non lo rispetterà, nella misura in cui la legge statunitense lo consenta. Audit periodici confermano l'adeguatezza della sicurezza dei dati ivi concordata.</i>
<b>Sulla base delle risposte fornite sopra, valutati gli aspetti di potenziale criticità, il trasferimento è:</b>		<b>Consentito</b>	



**Punto 4: Valutare il rischio di accesso legale nella giurisdizione di destinazione**

*I seguenti fattori sono stati redatti per la legge degli Stati Uniti*

a)	Valutare la probabilità che durante il periodo di valutazione, i seguenti argomenti legali impediscano alle autorità locali nella giurisdizione di destinazione (USA) di costringere con successo l'importatore/destinatario dei dati, a divulgare i dati personali in questione ai sensi delle leggi locali pertinenti come indicato nella precedente fase 2			
		<i>Probabilità</i>	<i>Probabilità che una possibile richiesta venga accolta</i>	<i>Analisi</i>
	L'importatore/destinatario dei dati non è un "fornitore di servizi di comunicazione elettronica" per quanto riguarda il trattamento dei dati personali in questione e, quindi, al di fuori dell'ambito di applicazione delle leggi pertinenti	0%	100,00%	<i>Nel contesto del trasferimento, l'importatore fornisce servizi cloud, di archiviazione dei dati e/o di comunicazione.</i>
	L'importatore/destinatario dei dati non ha alcun possesso, custodia o controllo sui dati personali in questione in chiaro e non può, pertanto, essere (con successo) ordinato di fornirli o consultarli in chiaro ai sensi delle leggi pertinenti	0%	100,00%	<i>L'importatore ha il possesso e la custodia dei dati.</i>
	Il trasferimento dei dati personali in questione o il contenuto dei dati personali saranno considerati comunicazioni a una persona situata negli Stati Uniti o a una persona statunitense, che potrebbero non essere "intenzionalmente mirate" dalle autorità statunitensi ai sensi delle leggi pertinenti	0%	100,00%	<i>L'importatore è una persona giuridica nella legislazione statunitense. Il trasferimento è quindi soggetto alle leggi pertinenti.</i>
	L'esecuzione di un accesso legale vietato violerebbe la legge dell'esportatore di dati in un modo non consentito dalla dottrina della cortesia internazionale della legge statunitense e che, quindi, impedisce tale richiesta	0%	100,00%	<i>Dato che i dati personali vengono effettivamente trasferiti e archiviati negli Stati Uniti, non è ipotizzabile che la dottrina della cortesia internazionale e l'applicabilità della legge europea sulla protezione dei dati impediscano un possibile accesso da parte del governo USA (in assenza di un nuovo accordo UE/USA che sostituisca il Privacy Shield).</i>
	Vi sono altri motivi giuridici, ai sensi del diritto statunitense, che impediscono un accesso legale vietato nel caso di specie	0%	100,00%	<i>Non vi sono motivi giuridici conosciuti dal titolare.</i>
b)	L'importatore/destinatario dei dati è contrattualmente tenuto a difendere i dati personali in questione da tentativi di accesso leciti?	Si	100,00%	<i>In base alle SCC dell'UE, che però da sole non sono sufficienti ad impedire l'accesso.</i>

c)	Probabilità che durante il periodo di valutazione, i dati siano considerati contenuti oggetto di richieste di accesso legittime, ai sensi delle pertinenti leggi locali, sulla base della probabilità di cui al punto 2	1,53%	1,53%	
d)	Possibilità tecnica, durante il periodo di valutazione, che l'importatore/destinatario dei dati sia tecnicamente in grado di applicare termini di ricerca (quali determinati destinatari o mittenti di comunicazioni elettroniche) senza l'autorizzazione dell'esportatore di dati, nell'ambito delle richieste di accesso legittime ai sensi delle pertinenti leggi locali?	100%	100,00%	<i>L'importatore ha accesso ai dati archiviati/custoditi e può quindi cercarli.</i>
f)	Sono in atto misure per scoprire se, durante il periodo di valutazione, le circostanze prese in considerazione nelle valutazioni di cui sopra non sono più valide?	Si		<i>L'esportatore monitora periodicamente lo sviluppo giuridico in questo settore (e almeno una volta all'anno). Inoltre, l'importatore di dati deve riferire di eventuali richieste di accesso legittime.</i>
Probabilità che gli argomenti legali non impediscano l'accesso legale straniero:			100,00%	} durante il periodo di valutazione
Probabilità annuale di un accesso legale vietato dalle leggi europee applicabili sulla protezione dei dati:			1,53%	
<b>In considerazione dei parametri TIA, il rischio residuo di accesso legale vietato è:</b>			Accettabile	
Numero di anni necessari affinché un accesso legale avvenga almeno una volta con una probabilità del 90% (calcolato con formula sulla base dei parametri inseriti):			747	
Numero di anni necessari affinché un accesso legale avvenga almeno una volta con una probabilità del 50% (calcolato con formula sulla base dei parametri inseriti):			225	
<i>supponendo che la probabilità non aumenti né diminuisca nel tempo</i>				
E' stata effettuata la valutazione nella fase 4 sulla base di quanto segue:		<i>Informazioni da parte dell'importatore dei dati, documentazione pubblica, quadro normativo di riferimento, parametri tecnici dei servizi</i>		

Punto 5: Conclusioni	
In considerazione di quanto sopra e della tipologia di dati trasferiti, il trasferimento è ritenuto dal Titolare:	Consentito
La presente valutazione d'impatto sui trasferimenti (TIA) è stata effettuata da:	<i>Titolare del trattamento, rappresentato dal Dirigente Scolastico</i>
Responsabile della TIA:	<i>Dirigente Scolastico</i>
Per il Responsabile della Protezione dei Dati (DPO):	<i>Dott. Anna CIMA</i>
<p>*Tutti i diritti relativi a questo foglio di calcolo e al metodo di valutazione dell'impatto del trasferimento sono riservati. Questo file è reso disponibile sotto una licenza Creative Commons libera "Attribuzione-Condividi allo stesso modo 4.0 Internazionale" (CC BY-SA 4.0) (<a href="https://creativecommons.org/licenses/by-sa/4.0/">https://creativecommons.org/licenses/by-sa/4.0/</a>). I campi di input e il testo di esempio in essi contenuti non sono soggetti alla licenza e possono essere modificati e condivisi. L'attribuzione deve anche includere il riferimento al link in cui è possibile ottenere la versione originale e master di questo file all'<a href="http://www.rosenthal.ch">www.rosenthal.ch</a>. Se hai bisogno di una licenza diversa, contattami all'indirizzo <a href="mailto:david@rosenthal.ch">david@rosenthal.ch</a>.</p>	

## Esito DPIA-TIA e conclusioni

La valutazione d'impatto svolta per l'utilizzo della piattaforma cloud, ha consentito di prendere in esame i vari aspetti del trattamento per valutarne eventuali criticità.

La correlazione tra le misure tecniche e organizzative adottate, le tipologie di rischi che si possono presentare, le probabilità che essi si verifichino e la gravità delle eventuali conseguenze, consente di giungere ad una "misurazione" del livello di rischio connesso al trattamento che, in conclusione di questa DPIA, può ritenersi Poco rilevante/Basso.

L'emergenza pandemica ha avuto, come unico effetto positivo, quello di far avviare un percorso di digitalizzazione che si è poi concretizzato in un ampliamento dell'offerta formativa, verso nuove metodologie di apprendimento e l'utilizzo delle nuove tecnologie, per migliorare la qualità dell'attività didattica. Questi strumenti hanno consentito di migliorare non solo l'ambito formativo, ma anche l'efficienza ed efficacia di tutto l'aspetto organizzativo didattico/amministrativo, tramite una più rapida condivisione dei documenti, la predisposizione di moduli che consentono di ottenere in tempo reale dati ed analisi, la calendarizzazione di tutti gli eventi immediatamente condivisibile, la creazione di gruppi di lavoro che possano efficacemente lavorare e coordinarsi anche a distanza.

La scelta dello strumento è stata fatta in pieno lockdown, quando era impellente attivare e garantire una nuova forma di continuità didattica nella maniera più semplice ed efficiente possibile, nel rispetto di parametri da cui la PA non può sottrarsi, come la scelta di servizi cloud abilitati da Agid (ora ACN). In quel contesto, il Ministero dell'Istruzione fornì delle indicazioni ed un elenco di servizi attivabili gratuitamente dalle scuole, tra cui è stato scelto quello che per conoscenza, affidabilità, sicurezza, facilità di utilizzo, diffusione è stato ritenuto più idoneo alle impellenti esigenze. Dal punto di vista del trattamento dati, il Garante privacy aveva emesso il provvedimento n.64 del 26 marzo 2020 "Didattica a distanza: prime indicazioni", nel quale indicava come non necessaria la DPIA e specificava che "L'Autorità vigilerà sull'operato dei fornitori delle principali piattaforme per la didattica a distanza, per assicurare che i dati di docenti, studenti e loro familiari siano trattati nel pieno rispetto della disciplina di protezione dati e delle indicazioni fornite dalle istituzioni scolastiche e universitarie". Il trasferimento dati extra UE verso gli Usa effettuato dalla piattaforma era legittimo in virtù del Privacy Shield, per cui non fu necessario affrontare alcuni aspetti dell'utilizzo della piattaforma.

Con la Sentenza Schrems-II, che ha invalidato il Privacy Shield, lo scenario è cambiato perché, pur non mutando niente sulla piattaforma in termini di affidabilità e sicurezza informatica, si è venuto a creare un vuoto normativo, una mancanza di adeguatezza rispetto al GDPR che di fatto rende il trasferimento dati in USA non conforme. La prima "reazione" della scuola è stata quella di limitarne l'uso solo ai docenti per attività organizzative e per lo svolgimento degli OOC da remoto (dovendo ancora mantenere misure di contenimento per la diffusione del Covid). Tuttavia, in assenza delle attese indicazioni del Garante privacy che potessero chiarire il quadro, specificare se e in che misura poter utilizzare questi servizi, con quali misure

ulteriori, in assenza del nuovo e annunciato accordo UE/USA per la regolamentazione del trasferimento dati, il titolare del trattamento si deve assumere la responsabilità di effettuare delle scelte in considerazione dei propri compiti istituzionali e del corretto svolgimento della propria attività.

Molti percorsi sono ormai già avviati attraverso l'uso di questa tecnologia e se alcune attività possono essere svolte ricorrendo a servizi e piattaforme diverse (es. l'uso di diverse caselle di posta, l'utilizzo del Registro elettronico per le comunicazioni), altre attività non possono prescindere dal ricorso alla piattaforma cloud oggetto della valutazione. Ci sono attività che le scuole devono svolgere necessariamente, e spesso in modalità remota, come le sedute degli OOCC (per mancanza di locali idonei a contenere un gran numero di persone), corsi di formazione specificamente previsti in modalità online (ad esempio nell'ambito delle misure del PNRR), e il tentativo di utilizzare strumenti alternativi ed open source (come ad es. GARR EduMeet) è stata fallimentare per numero di connessioni possibili, continuità e qualità del collegamento, possibilità di controllo sugli accessi.

La scuola si trova quindi a dover scegliere se continuare il suo percorso più innovativo rispetto al passato, previsto tra l'altro anche dal CAD con la transizione digitale delle PA per efficientare i servizi mentre il passaggio al cloud è uno dei principali obiettivi del Piano Nazionale Scuola Digitale nell'ambito delle misure del PNRR, oppure bloccare tutto e tornare indietro, annullando gli sforzi che docenti e alunni hanno fatto in questi anni. Su questa specifica piattaforma sono stati fatti investimenti di tempo, studio e lavoro (non economici perché è gratuita, con un risparmio tra l'altro per il bilancio di questo Ente) e anche con la volontà di migrare verso altre soluzioni cloud, che siano open source o proprietarie ma europee, la scuola non è riuscita a trovare soluzioni equivalenti per completezza e versatilità (oltre al fatto che alcune di esse utilizzano comunque servizi Google). A ciò si somma la considerazione che la piattaforma non sia messa in discussione per la sicurezza informatica o l'infrastruttura (possiede le maggiori certificazioni per gli standard internazionalmente riconosciuti ed è presente del Marketplace dell'ACN), ma che un vuoto normativo che dovrà essere colmato ne determina, nei fatti, una inadeguatezza formale rispetto alla normativa europea sul trattamento dati. Ed è chiaro che la portata della questione è sovranazionale, di natura politica ed economica, perché sono coinvolti due continenti e alcune delle maggiori società del digitale a livello mondiale (Google, Microsoft, Amazon, Meta, ...). Il Garante privacy, inoltre, non si è pronunciato sulla questione generale nonostante le tante sollecitazioni dal mondo istituzionale e produttivo del Paese, circoscrivendo il proprio intervento al solo servizio Google Analytics.

In relazione alla possibilità di accesso del Governo degli Stati Uniti ai dati della scuola, i numeri dimostrano come tale probabilità sia quasi nulla o comunque irrilevante, valutando oggettivamente improbabile che enti governativi possano essere interessati a tali dati per motivi di sicurezza nazionale. E anche ipotizzando che quel 1,53% possa verificarsi, l'entità e la tipologia di dati trattati tramite la piattaforma non sono tali da determinare rischi significativi per gli interessati, in considerazione anche del fatto che si tratta comunque di enti governativi e non di hacker con scopi illeciti.

Per quanto sopra esposto, analizzato, valutato, si ritiene che la piattaforma in oggetto possa essere utilizzata.

**Per il Titolare del Trattamento  
Il Dirigente Scolastico  
Dott.ssa Susanna Mustari  
f.to digitalmente ai sensi del CAD**