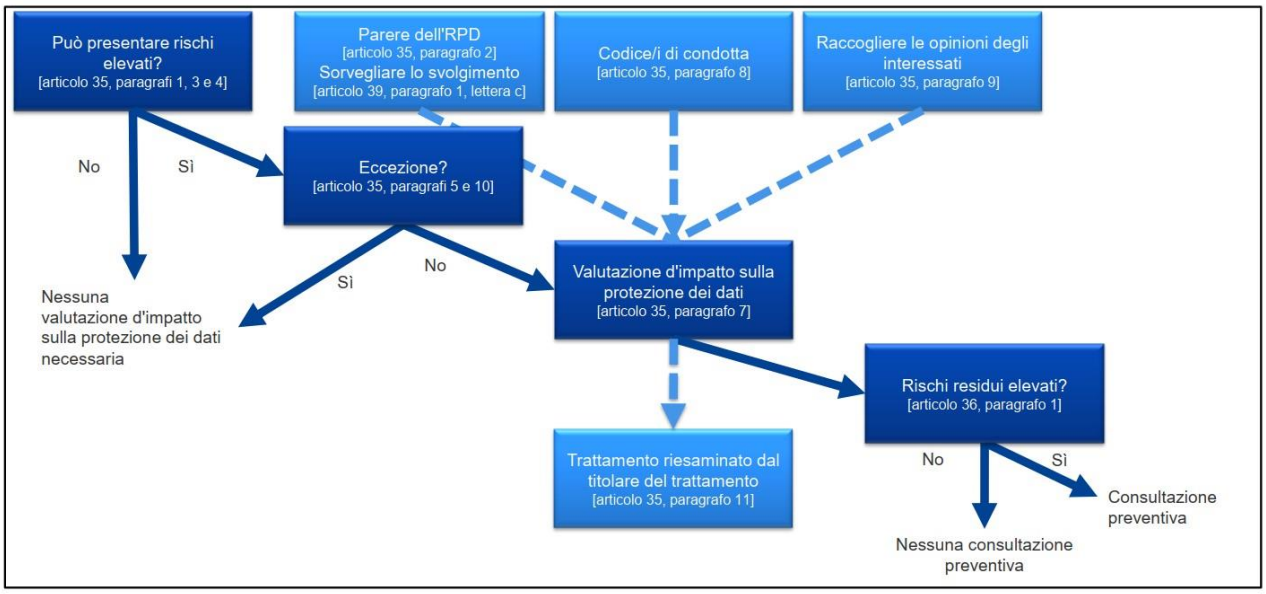
VALUTAZIONE D'IMPATTO SULLA PROTEZIONE DEI DATI (DPIA*) PER L'UTILIZZO DI PIATTAFORME CLOUD AI FINI DELLO SVOLGIMENTO DI ATTIVITA' DI DDI E AMMINISTRATIVE

Responsabile della Valutazione: D.S. – BIONDO SALVATORE
Posizione: Dirigente Scolastico a tempo indeterminato

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 trattamenti 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).



*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. La Valutazione è stata redatta con il supporto del DPO di questo Istituto.

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 aveva invalidato il Privacy Shield (Scudo privacy) e reso non conforme il trasferimento dati negli USA, il Titolare aveva limitato l'utilizzo della piattaforma per consentire comunque il corretto svolgimento delle attività di DDI oltre all'attuazione degli obiettivi stabiliti dal Piano Nazionale Scuola Digitale nell'ambito del PNRR, effettuando DPIA e TIA per valutare i rischi del trattamento.
Nel nuovo quadro normativo, che ha visto l'adozione dell'accordo UE-USA Data Privacy Framework a luglio 2023, si stabilisce che Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, per cui i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

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 OOCC 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 dalll'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 capacita 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 maniere 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 dai 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. 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, oltre ad essere certificato ai sensi del Dpf (Data privacy framework).

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

Si. La Commissione Europea, in virtù dei negoziati tra UE e USA che hanno portato all'adozione dell'accordo UE-USA Data Privacy Framework, è giunta alla conclusione che gli Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, con protezioni e garanzie sufficienti sul trattamento dei dati personali. Sulla base della nuova decisione di adeguatezza, i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

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=PxC

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

P	Probabilità di accadimento	C	Conseguenze
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:

Entità del rischio	Valori di riferimento
Poco rilevante	1≥ LR ≤3
Basso	4≥ LR ≤7
Alto	8≥ LR ≤12
Altissimo	13≥ LR ≤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 maniere 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/pesudonimizzati 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 OOCC, 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=PxC **LR**=2X2=**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=PxC **LR**=1X2=**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=PxC **LR**=2X2=**4** (in una scala che va da 1 a 16)

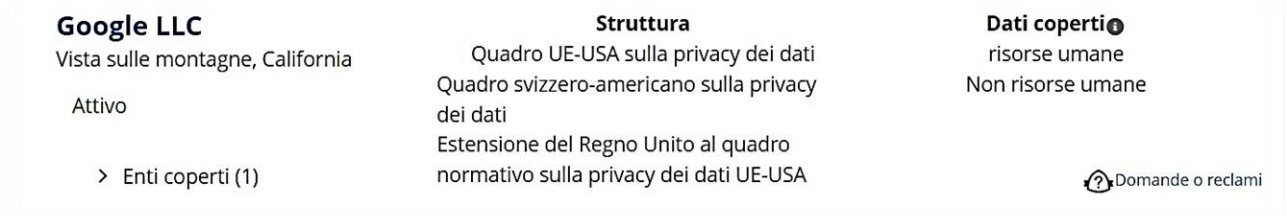
Livello di Rischio (LR)

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)

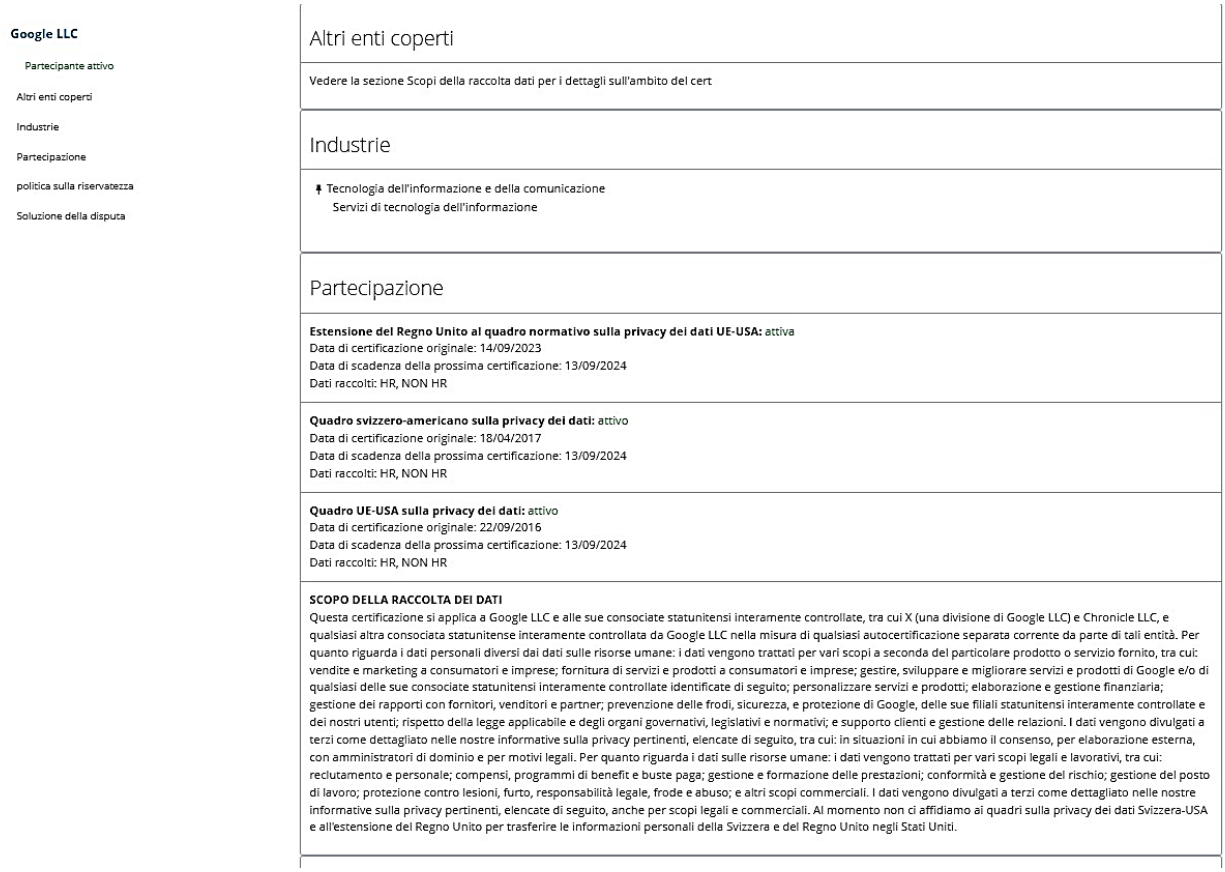
La TIA (Transfer Impact Assessment) è la valutazione dei rischi connessi al trasferimento dati extra UE, cioè al di fuori dello Spazio Economico Europeo (SEE). La redazione del documento, e quindi la valutazione di tali rischi, non è più necessaria con l'entrata in vigore dell'accordo UE-USA Data Privacy Framework, che ha stabilito che gli Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, con protezioni e garanzie sufficienti sul trattamento dei dati personali. Sulla base della nuova decisione di adeguatezza, i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati. Il titolare del trattamento, inoltre, ha verificato che il fornitore del servizio è certificato Dpf, cioè è inserito nella relativa lista e il trasferimento è coperto da tale certificazione.



È facile vedere, infatti, che:

- la certificazione è nello stato Attivo
- le Strutture di dati coperti sono quelle per i trasferimenti UE-USA, Svizzera-America, Regno Unito
- i Dati coperti da certificazione sono quelli Risorse umane (Dati personali relativi ai dipendenti di un'organizzazione, passati o presenti, raccolti nell'ambito del rapporto di lavoro) e Non risorse umane (Altri dati personali).

Entrando poi nel dettaglio del fornitore, è possibile verificare tutta una serie di altri requisiti e informazioni attraverso il menù a disposizione:



Esito DPIA 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 aveva invalidato il Privacy Shield, lo scenario era cambiato perché, pur non mutando niente sulla piattaforma in termini di affidabilità e sicurezza informatica, si era venuto a creare un vuoto normativo, una mancanza di adeguatezza rispetto al GDPR che di fatto rendeva 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 OOCC da remoto.
Nel nuovo quadro normativo, che ha visto l'adozione dell'accordo UE-USA Data Privacy Framework a luglio 2023, si stabilisce che Stati Uniti garantiscono un livello di protezione adeguato comparabile a quello dell'Unione europea, per cui i dati personali possono circolare in modo sicuro dall'UE verso le imprese statunitensi che partecipano al quadro, senza la necessità di ulteriori garanzie per la protezione dei dati.

Per quanto sopra esposto, analizzato, valutato, e in considerazione della certificazione Dpf del fornitore e del trasferimento dati, si ritiene che la piattaforma in oggetto possa essere utilizzata.

Per il Titolare del Trattamento
Il Dirigente Scolastico
Dott. Salvatore BIONDO