|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  | Risultati immagini per logo scuola viva |
| **ISTITUTO COMPRENSIVO**  **GIOVANNI PAOLO II**  Via E. Moscati, 4 84134 Salerno tel 089/751405  codice meccanografico SAIC8A6001 codice fiscale 95146370655  www.icgiovannipaolosecondosalerno.edu.it  e-mail: saic8a6001@istruzione.it – pec: [saic8a6001@pec.istruzione.it](mailto:saic8a6001@pec.istruzione.it)  codice univoco:UF5VI0 | | | |

**DPIA/TIA per** **l’adozione della piattaforma cloud GOOGLE WORKSPACE FOR EDUCATION per la gestione della DDI, delle comunicazioni interne e degli Organi collegiali a distanza per il trasferimento di dati verso paesi terzi in mancanza di decisione di adeguatezza**

### Richiesta parere degli interessati

Non è stato chiesto il parere degli interessati in quanto l’adozione della piattaforma cloud GOOGLE WORKSPACE FOR EDUCATION per la gestione della DDI, delle comunicazioni interne e degli Organi collegiali a distanza è finalizzata al perseguimento di un rilevante interesse pubblico e non si è pertanto ritenuto necessario richiedere un parere agli interessati. In ogni caso, la scuola si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto degli eventuali suggerimenti degli interessati.

# Contesto

## Panoramica del trattamento

### Questa DPIA si occupa della valutazione dell'impatto connesso all'uso della piattaforma cloud GOOGLE WORKSPACE FOR EDUCATION per la gestione della DDI, delle comunicazioni interne e degli Organi collegiali a distanza da parte degli studenti, delle loro famiglie, dei docenti e di altri dipendenti dell’istituzione scolastica.

### Attraverso l'utilizzo di strumentazione informatica quali tablet, smartphone e pc connessi in rete, costoro possono condividere informazioni e cooperare tramite sistemi di videocomunicazione, email e di condivisione documenti e risorse.

### Le applicazioni ritenute necessarie dalla scuola

### La piattaforma adottata dispone di applicazioni per la comunicazione e il lavoro collaborativo che possono essere utilizzati da alunni, docenti e altro personale per le attività didattico/formative, di comunicazione interna e gestione degli organi collegiali per le proprie finalità istituzionali. Ogni utente della piattaforma ha una sua identità digitale tramite una casella di posta elettronica personalizzata e rilasciata dalla scuola stessa.

### Con la propria identità digitale, ciascun utente registrato può utilizzare:

### Applicazioni di posta elettronica;

### Applicazioni di videocomunicazione;

### Applicazioni per la realizzazione e la condivisione di documenti;

### Applicazioni per la produzione e gestione di presentazioni;

### Applicazioni per la gestione delle lezioni;

### Applicazioni per la produttività personale e il lavoro collaborativo.

### Tali strumenti sono stati scelti sulla base di criteri di economicità, sicurezza, efficienza, facilità d’uso, protezione dei dati personali.

### Condizioni che richiedono una DPIA

### La scuola ha adottato la piattaforma cloud GOOGLE WORKSPACE FOR EDUCATION per la gestione della DDI, delle comunicazioni interne e degli Organi collegiali durante il periodo emergenziale dovuto al COVID 19, tenuto conto delle indicazioni del MIUR, del Garante della Privacy e dell’Agid in proposito.

### Considerata l’importanza oggi assunta dai trattamenti operati sulle piattaforme cloud per lo svolgimento delle attività istituzionali la scuola ha già provveduto a redigere un Data Privacy Impact Assessment (DPIA). Vista la recente approvazione da parte della Commissione Europea del US-EU Data Privacy Framework, accordo che stabilisce l’adeguatezza agli standard stabiliti dal GDPR dei trattamenti operati da aziende statunitensi certificate US-EU Dpf, procediamo ad aggiornare la presente DPIA alla luce di tale accordo.

### Finalità del trattamento

### La base giuridica dei trattamenti operati per le attività sopra menzionate è costituita dall’ esecuzione di un compito di interesse pubblico di cui è titolare la scuola (art. 6 comma 1 lettera e del GDPR), per l’attuazione del D. Lgs 82/2005 (CAD), la transizione digitale delle pubbliche amministrazioni, vista come strumento per contenere i costi e garantire una migliore efficienza dei servizi.

### E’ necessario richiedere il consenso per l’utilizzo della piattaforma?

### In considerazione dell’interesse pubblico perseguito non è necessario richiedere il consenso al trattamento da parte degli interessati. D’altronde la negazione del consenso, ove richiesto, impedirebbe alla scuola di conseguire le proprie finalità istituzionali. Questo è anche il parere espresso dal garante nel provvedimento 26 marzo 202, n.64.

## Dati e applicazioni

### Dati trattati

### I dati trattati sono i seguenti;

### nome, cognome ed indirizzo email assegnato

### informazioni sul dispositivo

### sistema operativo in uso

### rete in uso

### indirizzo IP

### informazioni di LOG

### informazioni sulla posizione

### versioni delle applicazioni

### browser impiegato

### software per la lettura della posta impiegato

### lingua preferita

### dati ed informazioni caricate sulla piattaforma dagli utenti (materiali didattici, compiti ed esercizi svolti dagli studenti, testi delle mail, ecc.)

### Ciclo di vita del trattamento dei dati (descrizione funzionale)

I dati vengono trattati per il tempo in cui l’utente usufruisce dei servizi della scuola in qualità di dipendente/studente e vengono cancellati quando il rapporto con l’istituzione scolastica si interrompe per trasferimento o fuoriuscita dell’interessato. In ogni caso, i dati sono conservati nei tempi e nei modi indicati dalle Linee Guida per le Istituzioni scolastiche e dai Piani di conservazione e scarto degli archivi scolastici definiti dalla Direzione Generale degli Archivi presso il Ministero dei Beni Culturali.

### Le applicazioni che lavorano sui dati

Gli interessati possono accedere e utilizzare i seguenti servizi individuati come necessari allo svolgimento dell’attività scolastica:

* un’applicazione di condivisione di file e cartelle;
* un’applicazione di messaggistica *sincrona* e *asincrona* (ad es. mail, chat, ecc.);
* un’applicazione di gestione delle classi virtuali;
* un’applicazione di editing e condivisione di documenti, fogli di calcolo e presentazioni;
* un’applicazione per la condivisione di calendari scolastici o di classe.

# Trasferimento dati extra UE

### Trasferimento di dati al di fuori dell'Unione europea

I dati oggetto del trattamento, registrati in sistemi informativi in Web cloud, NON sono conservati e/o trasferiti su server ubicati all'interno dell'Unione Europea oppure la loro ubicazione non è nota, pertanto si può garantire che siano rispettati pienamente tutti i diritti che il GDPR riconosce agli interessati dopo l’approvazione in data 10 Luglio 2023 del Data Privacy Framework da parte della Commissione Europea. Il Data Privacy Framework stabilisce che gli Stati Uniti d’America garantiscono un livello di protezione adeguato al trasferimento dei dati personali dei cittadini europei alle aziende d’Oltreoceano e paragonabile a quello dell’Unione Europea. Ciò rende pienamente conformi al GDPR il trasferimento di dati personali verso aziende che, come Google, sono certificate Dpf.

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

Sì. In base alla legislazione attuale il trattamento dei dati operati negli USA garantisce un livello di protezione equivalente al GDPR. Ciò a seguito dell’approvazione dello US-EU Data Privacy Framework.

Infatti, il trasferimento dei dati sui sistemi Google avviene sulla base di una dichiarazione di adeguatezza (art. 45 GDPR).

### Le condizioni contrattuali sottoscritte forniscono garanzie di adeguatezza ex art. 46 GDPR ?

Google rassicura i suoi clienti ed utenti riguardo ai trattamenti operati sui dati rimandando al Cloud Data Processing Addendum (CDPA) reperibile all’indirizzo: <https://cloud.google.com/terms/data-processing-addendum>. Qui, all’art.10, si garantisce che se il trasferimento dei dati personali avviene verso un Paese non coperto da una decisione di adeguatezza, vengono applicate le clausole contrattuali tipo, come previsto dall’art. 46 del GDPR, cui i clienti possono aderire sottoscrivendole insieme all’Emendamento sul trattamento dei dati.

### Il trasferimento è necessario per importanti motivi di interesse pubblico (art. 49, par. 1. Lett. d del GDPR)?

### Si. La base giuridica dei trattamenti operati è l’ esecuzione di un compito di interesse pubblico (art. 6 comma 1 lettera e del GDPR).

### L’uso della piattaforma Google Workspace for Education è finalizzato non solo al perseguimento delle finalità istituzionali di istruzione e formazione ma anche a perseguire gli obiettivi della transizione digitale imposta alle PA dal D. Lgs 82/2005 (CAD) e seguenti.

### E’ possibile perseguire l’interesse pubblico con altri strumenti?

### E’ indubbio che il perseguimento delle finalità istituzionali prima richiamate debba tener conto delle condizioni di realtà e, in particolare, di mercato nel quale vi sono alternative alla piattaforma di Google oggetto di questo documento, ma queste non presentano le stesse garanzie di affidabilità e sicurezza informatica..

### Considerando le limitate risorse economiche e tecniche di cui la nostra scuola è dotata, neanche le analoghe piattaforme open source, pur oggetto di norme e incentivi da parte delle autorità di indirizzo, possono essere prese in considerazione per la loro limitatezza, in quanto ai servizi e alla loro integrazione, oltre che sicurezza informatica. Pertanto, si ritiene che l’adozione di simili piattaforme renderebbe nello stesso tempo i dati più vulnerabili.

### D’altra parte, non si può pensare di interrompere il processo di innovazione che lo stato emergenziale da COVID 19 ha impresso alla PA ed, in particolare, alle scuole come la nostra.

### Le nuove tecnologie e la piattaforma cloud adottata sono quindi oggi indispensabili al perseguimento degli interessi pubblici e la nostra scuola non può rinunciare ad esse senza rinunciare a perseguire le proprie finalità istituzionali.

### Quali misure supplementari sono state adottate?

### Si ritiene, pertanto, di dover adottare il principio di minimizzazione del rischio stabilito, non prima di aver valutato l’inesistenza di possibili soluzioni alternative che offrano maggiori garanzie di adeguatezza.

### In pratica, la nostra scuola si impegna ad adottare misure supplementari per ridurre il rischio associato all’uso della piattaforma GOOGLE per poi misurare l’entità del rischio residuo e valutare se è al di sotto di una soglia che si può ritenere accettabile.

### Si precisa che le misure supplementari prese in considerazione sono misure realisticamente attuabili dalla nostra scuola nel contesto economico/tecnico di cui si è già detto.

### Le misure di contenimento dei rischi che sono state prese in considerazione sono, in sequenza:

### Coinvolgimento del DPO nella presente valutazione;

### Attenta valutazione e scelta dei dati da trattare, in base ai principi di necessità (per i dati sensibili) e di riduzione del rischio (per i dati comuni);

### Valutazione dei servizi necessari per la minimizzazione dei rischi;

### Attribuzione dei ruoli per individuare specifici ruoli e responsabilità.

### Pseudonimizzazione dei dati sensibili per garantire adeguati livelli di protezione;

### Definizione di un regolamento interno per l’uso della piattaforma.

### Il DPO è stato coinvolto nella valutazione dei rischi?

Si. Il DPO ha fornito supporto ed assistenza nella redazione del presente documento e degli altri documenti a supporto.

### Ruoli e responsabilità

### Sono stati attribuiti i seguenti ruoli e relative responsabilità:

### **Titolare del trattamento:** in questo caso il Dirigente Scolastico (DS), legale rappresentante della scuola, assume il ruolo di supervisione e guida nei confronti dell'operato dei docenti e di tutte le parti in causa.

### **Docenti:** hanno funzioni di supervisione relativamente alle attività didattiche da loro gestite.

### **Consiglio di classe:** composto dai docenti e dalle altre componenti, utilizza la piattaforma per gli scopi istituzionali.

### **DPO:** ha il compito di fornire supporto al DS e agli altri utenti per tutte le questioni riguardanti la protezione dei dati personali.

* **Responsabili del trattamento:** i fornitori dei servizi in cloud utilizzati che debbono 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.

### **Eventuali amministratori di sistema**: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici..

### Principio di minimizzazione dei dati personali trattati

Per ridurre i rischi associati si limita il trattamento ai soli dati necessari per il conseguimento delle finalità sopra richiamate.

In particolare la scuola utilizza per ogni utente soltanto il nome ed il cognome dell’interessato a cui viene poi attribuita la casella istituzionale costituita da [nome.cognome@dominioscuola.it](mailto:nome.cognome@dominioscuola.it).

E’ disabilitata la possibilità di aggiungere ulteriori informazioni da parte dell’utente proprietario del profilo.

Analogamente, nei documenti opportuni, sono state impartite istruzioni ai diversi utilizzatori per minimizzare i dati trattati nei loro procedimenti.

### Adozione di misure per il trattamento di dati sensibili

### Il trattamento dei dati sensibili è stato generalmente vietato, salvo che per le attività indispensabili e istituzionali della scuola, in particolare per la redazione e la condivisione di documenti quali, ad esempio, il Piano Educativo Individualizzato (PEI) o il Piano Didattico Personalizzato (PDP). In tal caso, la scuola ha deciso di permettere la redazione e lo scambio di tali documenti (quando indispensabile e non possibile con altri mezzi) in forma pseudonimizzata a seguito dell’associazione di un codice personalizzato e riservato per ogni alunno che necessita della redazione del documento.

### Principio di minimizzazione in relazione alle applicazioni utilizzate

Si. Nella scelta dei servizi e delle applicazioni utilizzate si sono selezionate solo le applicazioni ed i servizi strettamente indispensabili come già richiamato precedentemente, tenendo conto dei principi di necessità e di minimizzazione.

### Tecniche di anonimizzazione, pseudonimizzazione e cifratura per la protezione dei dati personali

Sono state adottate solo misure di pseudonimizzazione come indicato nei paragrafi precedenti per i soli dati sensibili.

Non sono state adottate altre misure, quali quelle di anonimizzazione o cifratura perché si è valutato che non avrebbero aumentato la sicurezza complessiva dei trattamenti, per la eccessiva complessità di gestione in relazione al contesto, anche in considerazione della inadeguatezza tecnica da parte della maggior parte dell’utenza (studenti, ma anche docenti, ad esempio).

### Idonea informativa fornita agli utenti e procedure di utilizzo della piattaforma

Si. Alla informativa generale rivolta agli studenti, alle loro famiglie, ai docenti, al personale scolastico ed ai consulenti che hanno rapporti con gli studenti nell’ambito di attività formative extra curriculari è stato fornito un addendum specifico alla informativa a loro dedicata con specifiche informazioni relative al trattamento in questione.

Inoltre, sono stati edotti con riguardo alle procedure di utilizzo tramite il regolamento d’uso interno della piattaforma.

### E’ stato definito un parametro di rischio accettabile (KPI) relativamente all’accesso non autorizzato sui dati della piattaforma da parte del governo USA in violazione del GDPR?

È stato definito un KPI specifico, facendo riferimento alla probabilità massima di accesso annuale accettabile in violazione del GDPR. Si considera accettabile una probabilità di 1 accesso ogni 10 anni su una popolazione scolastica media annuale di 800 elementi. In tal caso, ciò corrisponde ad una probabilità di accesso di 125 su un milione di individui.

### Probabilità che si verifichi un accesso non autorizzato sui dati della piattaforma da parte del governo USA in violazione del GDPR

Per valutare la probabilità che si verifichi un accesso non autorizzato da parte delle autorità statunitensi si sono considerate le statistiche di tale evento disponibili all’url <https://transparencyreport.google.com/user-data/overview> calcolando un numero di account iscritti a Google Workspace nel 2021 di circa 3 miliardi.

Considerando che il numero di accessi non autorizzati da parte del governo USA sono necessariamente inferiori a quelli da parte di qualsiasi governo nel mondo (dati 2021 riportati nel report segnalato), si calcola una probabilità da parte di qualsiasi governo pari a 101 su un milione di individui. Pertanto, la probabilità di accesso da parte del governo USA dovrà essere sensibilmente inferiore.

### Rischio associato al trasferimento dei dati al di fuori dell’UE

Dall’analisi effettuata, rispetto all’obiettivo assegnato, il rischio associato al trasferimento dei dati al di fuori dell’UE risulta essere accettabile.

Al fine di verificare e garantire nel tempo che questo rischio continui a mantenersi accettabile, si provvederà a verificarne la validità con cadenza annuale.

### Conclusioni sulla valutazione del rischio associato al trasferimento extra UE dei dati personali

Il rischio associato al trasferimento extra UE dei dati trattati è stato ragionevolmente valutato per il momento come contenuto e accettabile, a maggior ragione che qui si tratta di dati relativi alla popolazione e al contesto scolastici, per cui ci si aspetta che tali dati siano ancor di più meno significativi per i governi extra UE.

# Principi Fondamentali

## Proporzionalità e necessità

### Con riferimento a questa sezione della DPIA, si ricorda che le uniche motivazioni che ci hanno indotto ad effettuarla sono poichè l'attività di trattamento comporta il trattamento di dati sensibili quali quelli trattati nei documenti PDP, PEI, ecc. e contemporaneamente relativi a soggetti fragili quali minori, nonostante il parere contrario del Garante della Privacy che non l’ha ritenuta necessaria per le scuole.

### Pertanto, nel fare riferimento specifico a quanto riportato negli altri documenti relativi ai trattamenti effettuati (informative, addendum, registro dei trattamenti , ecc.), oltre a quanto già precisato relativamente alle motivazioni sopra riportate che ci hanno indotto alla DPIA, si ribadisce che:

### **Gli scopi del trattamento sono specifici, espliciti e legittimi**: la gestione delle attività didattico/formative, anche per via telematica, la comunicazione interna tra le varie figure della scuolae la gestione degli organi collegiali, anche per via telematica.

### **Le basi legali che rendono lecito il trattamento** sono esplicitate nell’informativa generale fonita ai soggetti interessati (studenti e loro famiglie, docenti e altri dipendenti della scuola, consulenti che abbiano rapporti con gli studenti per progetti formativi extra curriculari, ecc.).

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

### **I dati sono esatti e aggiornati**: i dati trattati sono per la natura stessa dei trattamenti dati dinamici perché oggetto di lavoro cooperativo (in genere didattico) da parte degli interessati.

### **Il periodo di conservazione dei dati** è quello indicato nell’informativa generale, secondo i termini ella normativa vigente.

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

### Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 206/679.

### Non viene richiesto il consenso agli interessati perché il trattamento si basa su una funzione di interesse pubblico del titolare.

### La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti di accesso, rettifica cancellazione, limitazione, opposizione.

### I trattamenti operati da Google sono regolamentati dal Cloud Data Processing Addendum (CDPA) dove sono specificati gli obblighi del fornitore individuato responsabile del trattamento. Vi sono dei limiti realistici a tali obblighi per la differente “forza” contrattuale tra la scuola e il fornitore, di cui si è precedentemente già discusso.

# Rischi

## Misure esistenti o pianificate

### Crittografia: Il fornitore cripta i dati per impostazione predefinita;

### Controllo degli accessi logici tramite un sistema di login e password;

### Minimizzazione dei dati, come precedentemente illustrato;

### Archiviazione tramite opportune procedure gestite nei tempi richiesti dalla norma;

### Lotta contro il malware, attraverso sistemi software antivirus e procedure;

### Backup garantito dal fornitore;

### Manutenzione: effettuata dall’amministratore di sistema che garantisce anche la gestione e la sicurezza dei sistemi informatici, oltre che dal fornitore per la disponibilità e tenuta generale del sistema;

### Contratto con il responsabile del trattamento, come precisato più volte in precedenza;

### Politica di tutela della privacy: istruzioni specifiche e regolamenti sono stati emanati dalla scuola.

## Valutazione del rischio

Riportiamo di seguito la valutazione della gravità dei seguenti rischi associati all’uso della piattaforma:

* Accesso illegittimo ai dati
* Modifiche indesiderate ai dati
* Perdita di dati

Prima di valutare l’entità del rischio procederemo alla stima dei seguenti fattori:

entità del danno: 1. Trascurabile, 2. Limitata, 3. Importante, 4. massima

probabilità del rischio: 1. Trascurabile, 2. Limitata, 3. Importante, 4. Massima

L’entità del rischio sarà quindi un valore compreso fra 1 e 16 determinato come il prodotto fra entità del danno e la probabilità del rischio.

## Accesso illegittimo ai dati

### Tale rischio può essere dovuto a:

### errori nell’indicazione dell’indirizzo del destinatario di una comunicazione, oppure all’errato uso del campo CC al posto di quello CCN;

### errori nella concessione dei permessi di accesso ai documenti;

### azioni dolose da parti di utenti della piattaforma o di estranei.

### **Misure atte a mitigare il rischio**:

### controllo degli accessi logici;

### minimizzazione dei dati;

### pseudonimizzazione;

### formazione degli utenti.

### manutenzione;

### politiche di tutela della privacy.

### Stima gravità del danno:possiamo ritenere limitata (livello 2 su una scala di 4) la gravità del danno per l’accesso illegittimo ai dati comuni mentre più grave va considerato l’accesso illegittimo ai dati di natura sensibile come nel caso eventuale di documenti PDP/PEI. In questo caso la gravità del rischio può essere stimata come importante (livello 3 su una scala di 4).

### Stima probabilità del rischio:A seguito delle misure di sicurezza adottate la probabilità del rischio può essere valutata come limitata (livello 2 su una scala di 4).

### Stima gravità del rischio:

### Gravità del rischio accesso illegittimo ai dati: 3x2=6 (valore massimo 16)

## Modifiche indesiderate dei dati

### Il secondo rischio è la modifica indesiderata di dati che può essere dovuta a:

### errore umano;

### azione dolosa.

### Misure atte a mitigare il rischio:

### controllo degli accessi logici;

### lotta contro i malware;

### backup;

### formazione degli utenti;

### manutenzione;

### politiche di tutela della privacy.

### Stima gravità del danno:possiamo ritenere limitata (livello 2 su una scala di 4) la gravità del danno.

### Stima probabilità del rischio:A seguito delle misure di sicurezza adottate la probabilità del rischio può essere valutata come trascurabile (livello 1 su una scala di 4).

### Stima gravità del rischio:

### Gravità del rischio modifiche indesiderate dei dati: 2x1=2 (valore massimo 16)

## Perdita di dati

### Il terzo rischio che andiamo a valutare è la perdita di dati dovuta a:

### errore umano;

### malfunzionamenti della piattaforma o guasti;

### azione dolosa;

### Misure atte a mitigare il rischio: tutte le misure adottate e citate al punto precedente sono atte a mitigare il rischio. Fra le più pertinenti citiamo:

### controllo degli accessi logici

### archiviazione e backup

### manutenzione

### politiche di tutela della privacy

### lotta contro i malware

### formazione

### procedure per la gestione degli incidenti

### Stima gravità del danno:possiamo ritenere limitata (livello 2 su una scala di 4) la gravità del danno.

### Stima probabilità del rischio:A seguito delle misure di sicurezza adottate la probabilità del rischio può essere valutata come trascurabile (livello 1 su una scala di 4).

### Stima gravità del rischio:

### Gravità del rischio perdita dei dati: 2x1=2 (valore massimo 16)

## Valutazione gravità del rischio

|  |  |  |  |
| --- | --- | --- | --- |
| **Rischio** | **Entità del danno** | **probabilità** | **Gravità del rischio** |
| Accesso illegittimo ai dati | 3 | 2 | 6 |
| Modifiche indesiderate ai dati | 2 | 1 | 2 |
| Perdita di dati | 2 | 1 | 2 |

### L’analisi condotta evidenzia come i rischi siano al di sotto di una soglia accettabile.