ISTITUTO COMPRENSIVO "CASOPERO- FILOTTETE"
INDIRIZZO: VIA DELLA LIBERTA' 60 – 88811 CIRO'MARINA (KR)
Cf: 91021410799 **Meccanografico**: KRIC82400D
Email: KRIC82400D @istruzione.it **Pec**: KRIC82400D@pec.istruzione.it

AGGIORNAMENTO DIPIA 13/01/2025

Autore:
Daniele Perrotta

Redattore:
Daniele Perrotta

Nome del DPO/RPD
DATAMAT Srls

Parere del DPO/RPD
I rischi residui, a seguito delle misure di sicurezza intraprese, sono congrui alle finalità del trattamento.

Richiesta del parere degli interessati
Non è stato chiesto il parere degli interessati.

Motivazione della mancata richiesta del parere degli interessati
Non si è ritenuto necessario richiedere un parere agli interessati, anche vista l'urgenza connessa. Qualora vi fossero suggerimenti da parte dell'utenza, l'amministrazione si impegna ad effettuare successivi aggiornamenti della presente DPIA che tengano conto degli stessi.

Contesto

Panoramica del trattamento

Quale è il trattamento in considerazione?
Questa DPIA è atta alla valutazione dell'impatto connesso all'uso di tecniche di insegnamento da remoto, tramite l'utilizzo di tecnologie digitali.
Questa tecnica di insegnamento comporta la fruizione di processi formativi da parte degli alunni tramite l'utilizzo di strumentazione informatica, anche personale, quali tablet, smartphone e pc connessi in rete.
La fruizione di tali processi può avvenire in ambito sia scolastico che domestico, e prevede l'utilizzo di tecnologie online di condivisione e cooperazione finalizzate al raggiungimento di un obiettivo del singolo alunno e/o del gruppo di lavoro.
L'utilizzo di meccanismi di condivisione e cooperazione facenti uso di tecnologie cloud, però, è associabile ad un rischio connesso al trattamento dei dati personali degli alunni. Si rende perciò necessaria l'identificazione di piattaforme e policy di utilizzo volte a minimizzare la possibilità di violazioni della privacy degli studenti.

Quali sono le responsabilità connesse al trattamento?
La complessità delle azioni e dei possibili risvolti in termini di violazione della privacy implica una collaborazione fattiva tra le varie parti in causa. Queste sono, in particolare:

- **Il titolare del trattamento, in questo caso l'Amministrazione Scolastica, rappresentata legalmente dal Dirigente Scolastico (D.S.), che assume un ruolo centrale di supervisione e guida nei confronti dell'operato dei docenti. Inoltre, è compito del D.S. quello di definire un codice di condotta interno alla scuola che regoli l'utilizzo della strumentazione elettronica utilizzata, e di sorvegliare sulla sua attuazione.**
- **I docenti. Il loro ruolo centrale nella produzione di compiti e contenuti deve essere associato ad un loro controllo nei confronti di tutte quelle attività suscettibili di violazioni della privacy. Al loro ruolo di amministratori, spesso unici, di tutta la documentazione accessibile ai gruppi di lavoro va associata la responsabilità del controllo delle regole di utilizzo prescritte, e la vigilanza sul corretto svolgimento delle operazioni. A tal fine, il titolare si impegna ad attribuire ai docenti il compito di supervisione sulle attività didattiche su piattaforma informatica e a fornire agli stessi indicazioni sulle modalità più opportune con cui trattare i dati personali, ai fini dell'Art. 2-quaterdecies del D.Lgs. 196/2003.**
- **Il consiglio di classe (o di interclasse per la scuola primaria): Delibera sulla valutazione finale in fase di scrutini. Potrebbe quindi essere necessario allo stesso l'accesso ai documenti presenti sulla piattaforma informatica, ivi inclusi i dati personali.**
- **Il Responsabile della Protezione dei Dati (RPD) ha il compito di fornire supporto a titolare, docenti e interessati, per tutte quelle questioni concernenti la protezione dei dati personali all'interno dell'ambito di applicazione del trattamento.**
- **I responsabili del trattamento, quali i provider di servizi elettronici utilizzati per la didattica (eventualmente, BYOD) devono 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. Particolare attenzione va posta nei confronti dei fornitori di servizi cloud, ove richiesti. In questo caso, è necessario prestare particolare attenzione alle loro policy sulla cessione dei dati a organismi terzi e all'eventuale salvataggio di dati su server extra-UE. Per questo motivo, sarà necessario effettuare una valutazione preventiva dei provider di servizi Cloud sulla base della loro compliance nei confronti della normativa in essere. Inoltre, sarà necessario procedere alla nomina formale dei fornitori di tali servizi quali responsabili del trattamento ai sensi dell'Art. 28, comma 3 del GDPR. Si ricorda inoltre che, sulla base di quanto previsto dalla circolare AGID n. 2 del 9 aprile 2018, le Pubbliche amministrazioni possono avvalersi esclusivamente di servizi cloud abilitati, la cui lista aggiornata può essere trovata sul sito dell'AGID.**
- **Eventuali amministratori di sistema: nominati dal DS quali responsabili del trattamento relativamente alla gestione dei sistemi informatici, collaborano con l'RPD e il DS nel fornire consulenze e pareri relativamente allo stato delle risorse informatiche dell'amministrazione.**

Ci sono standard applicabili al trattamento?

Attualmente non sono stati rinvenuti standard, certificazioni o codici di condotta applicabili al problema in esame. L'European Data protection Board (edpb) ha però recentemente pubblicato le *"Raccomandazioni 01/2020 relative alle misure che integrano gli strumenti di trasferimento al fine di garantire il rispetto del livello di protezione dei dati personali dell'UE"*, che specificano i comportamenti da seguire riguardo al trasferimento di dati all'estero, che potrebbe essere rilevante per il trattamento in oggetto.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

La didattica da remoto utilizza gli strumenti di collaborazione digitale per il perseguimento di finalità didattiche e formative. Nel caso specifico gli strumenti hardware, anche di proprietà degli studenti, vengono utilizzati con l'intento di svolgere compiti didattici o per l'accesso a materiale formativo.
Le attività didattiche sono quindi svolte tramite una o più piattaforme elettroniche che facilitano la condivisione dei dati e l'organizzazione del lavoro di gruppo. Tali piattaforme, che spesso fanno utilizzo di tecnologie *cloud*, si troveranno quindi a contenere, oltre alle informazioni necessarie per identificare univocamente alunni, docenti ed eventuali altri interessati, tutta una serie di dati e informazioni da essi prodotti, che perlopiù potrebbero essere condivisi tra diverse parti in causa, specialmente durante la loro stesura nel caso di progetti di didattica cooperativa.
Tali informazioni dipenderanno ovviamente dalla natura e materia didattica svolte, ma potrebbero contenere dati o informazioni ad alto rischio per la privacy degli interessati. A titolo di esempio, potrebbero contenere degli scritti che definiscono esplicitamente l'orientamento politico, la razza o la condizione sanitaria degli interessati, che potrebbero essere di minore età. E' quindi importante sensibilizzare tutti gli utenti (alunni e docenti) sulla necessità di limitare allo stretto indispensabile la presenza di dati sensibili e di attuare comunque un principio di minimizzazione dei dati personali, anche comuni. Infine, è importante far notare che i dati presenti nelle piattaforme potranno essere oggetto di valutazione scolastica.

Qual'è il ciclo di vita del trattamento dei dati (descrizione funzionale)?
L'intero ciclo di vita dei dati passa attraverso alcune fasi che presentano dei rischi potenziali. In particolare, gli studenti sono invitati a registrarsi a uno o più servizi di condivisione e organizzazione didattica, tramite l'utilizzo di uno o più dispositivi di loro proprietà o forniti in comodato dalla scuola. Per quanto riguarda la piattaforma G Suite è la scuola che provvederà a realizzare le utenze da assegnare a docenti e studenti ed utilizzate per lo svolgimento dell'attività didattica.
Durante le attività didattiche tali servizi saranno utilizzati per affidare agli studenti dei compiti, a volte da svolgere in team, che prevedono la produzione di materiale. Tale materiale verrà con tutta probabilità conservato su server cloud e condiviso tra i vari membri del team. Alla fine della produzione dello stesso, si potrà procedere all'archiviazione del materiale da parte dei docenti interessati, che ne potrebbero fruire all'atto di esprimere (ed eventualmente di giustificare) una valutazione sull'operato degli studenti. A tal fine, la documentazione ottenuta si profila quale atto amministrativo endoprocedimentale. Per questo motivo è evidente come sia compito del docente procedere all'archiviazione dei documenti nel momento in cui non sia più necessaria alcuna modifica da parte degli alunni. L'archiviazione dovrà essere effettuata in modo tale da rendere non accessibile la documentazione agli interessati, che potranno averne accesso o richiederne la modifica, rettifica o cancellazione solamente tramite richiesta scritta che non limiti le finalità del trattamento, orientate al corretto svolgimento dell'attività didattica.
Per quanto riguarda la cancellazione dei dati, la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" prescrive la conservazione di elaborati delle prove scritte, grafiche e pratiche per almeno un anno, e la conservazione di documentazione campione un anno ogni dieci (si suggerisce per omogeneità di non scartare i documenti relativi agli anni scolastici terminanti in 7/8, es. '67/'68, '77/'78 etc.).

Quali sono le risorse di supporto ai dati?
Solitamente ci si avvale di servizi in *cloud* che permettono la condivisione e organizzazione dei compiti assegnati. Tali tecnologie possono, talvolta, basarsi su server extra-ue, e in tal caso è importante verificarne la compliance alla normativa europea sul trattamento dei dati.

A causa delle qualità *cross-platform* di questi servizi, essi vengono fruiti dagli interessati tramite una grande varietà di strumentazione informatica che può comprendere tablet, pc e smartphone, che a loro volta possono essere basati su diversi sistemi operativi e permettere la fruizione dei servizi tramite diversi browser o app.

Principi Fondamentali

Proporzionalità e necessità

Gli scopi del trattamento sono specifici, espliciti e legittimi?

Il trattamento prevede l'utilizzo di tecniche didattiche innovative atte allo svolgimento dell'insegnamento scolastico in modalità remota e a sostenere un approccio consapevole al digitale nonché la capacità d'uso critico delle fonti di informazione degli studenti.

Lo scopo ultimo è quello di formare gli studenti, con l'effetto collaterale di aumentarne la consapevolezza nell'uso delle tecnologie moderne e nell'utilizzo di strumentazione digitale.
I dati personali relativi alle attività didattiche possono portare ad una valutazione degli studenti stessi da parte dei docenti e sono quindi suscettibili di diventare atti amministrativi scolastici.

Quali sono le basi legali che rendono lecito il trattamento?
Il trattamento viene effettuato sulla base del dpcm dell'8 marzo 2020 e successive modifiche ed aggiornamenti che prevedono l'attivazione di strumenti per lo svolgimento delle attività didattiche a distanza in sostituzione o ad integrazione dell'attività didattica in presenza.

Per gli elaborati degli studenti soggetti a valutazione è rilevante la Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche", che prescrive la conservazione di documentazione campione un anno ogni dieci (si suggerisce per omogeneità di non scartare i documenti relativi agli anni scolastici terminanti in 7/8, es. '67/'68, '77/'78 etc.).

Trattandosi di soggetti di minore età, è bene ricordare che alla luce del D.L. 101 del 10 agosto 2018 (art. 2 - quinquies), l'età dalla quale il minore "può esprimere il consenso al trattamento dei propri dati personali in relazione all'offerta diretta di servizi della società dell'informazione" è stata fissata a 14 anni. In ogni caso la base legale del trattamento non è il consenso dell'interessato ma un obbligo di legge cui è soggetto il titolare del trattamento.

I dati raccolti sono adeguati, pertinenti e limitati a quanto è necessario in relazione alle finalità per cui sono trattati (minimizzazione dei dati)?
I docenti sono invitati a raccogliere (e archiviare) la quantità minima di dati personali necessaria al corretto svolgimento delle loro funzioni. Particolari restrizioni dovranno essere adottate per i dati sensibili che dovranno limitarsi a quelli strettamente necessari.
Ciò nonostante, è importante far notare come un corretto giudizio sul processo formativo degli studenti passi attraverso l'attenta valutazione dell'intero processo formativo dello studente, e non soltanto dell'elaborato ottenuto nella sua fase finale. Per questo motivo, tutte le informazioni legate al processo

formativo possono essere considerate pertinenti ai fini della valutazione e quindi oggetto del trattamento.

I dati sono esatti e aggiornati?
La procedura di raccolta e conservazione dei dati prevede la creazione spesso cooperativa di contenuti, perciò potrebbe presentarsi il caso in cui un elaborato venga deliberatamente modificato da eventuali collaboratori durante il suo processo di creazione. In tal caso, è preferibile utilizzare uno strumento che tenga traccia delle modifiche apportate alla documentazione, tramite ad esempio soluzioni di backup e di cronologia delle modifiche.
Una volta terminati, gli elaborati delle prove scritte, grafiche e pratiche possono essere considerati documentazione amministrativa oggetto di valutazione scolastica. Per questo motivo, essi non possono essere modificati o cancellati neppure su richiesta degli interessati per il periodo prescritto dalla legge e comunque funzionale alla corretta valutazione da parte dei docenti e del consiglio di classe.

Qual è il periodo di conservazione dei dati?
La conservazione dei dati è necessaria per un periodo strettamente necessario allo svolgimento dell'attività formativa. successivamente ad essa, i dati verranno archiviati dal docente (anche attraverso una apposita funzionalità proposta dal servizio, ove presente), e la documentazione prodotta verrà resa inaccessibile agli interessati, salvo richiesta scritta di accesso o cancellazione degli interessati.
Nel caso in cui gli elaborati debbano essere oggetto di valutazione, l'archiviazione deve essere mantenuta per almeno un anno dalla produzione, a meno che non ci si trovi nei casi particolari previsti dalla Circolare n° 44 del 19/12/2005 della Direzione Generale per gli archivi - "Archivi delle Istituzioni Scolastiche" che prescrive la conservazione di documentazione campione un anno ogni dieci. In tal caso, bisogna distinguere i due casi:

- dati ed elaborati non soggetti a valutazione: non hanno necessità di essere conservati per eventuali verifiche o controlli per cui devono essere cancellati nel momento in cui termina l'attività formativa svolta. Di norma tali dati vanno cancellati alla fine dell'anno scolastico a meno che l'attività programmata si svolga su più anni scolastici ed è necessario per essa operare qualche forma di trattamento anche sui dati raccolti gli anni precedenti;
- dati ed elaborati soggetti a valutazione: il periodo di conservazione deve rispettare le disposizioni previste dalla legge fra cui la citata circolare n°44 del 19/12/2005 della Direzione Generale degli archivi-.

Misure a tutela dei diritti degli interessati

Come sono informati del trattamento gli interessati?
Gli interessati vengono informati del trattamento precedentemente all'inizio dello stesso, tramite somministrazione di informativa ex Art. 13 del Reg. UE 206/679. L'informativa viene somministrata ad alunni e genitori degli stessi tramite una combinazione più completa possibile dei canali disponibili alla scuola, che includono, a titolo esemplificativo e non esaustivo:

- La pubblicazione di una circolare;

- L'invio della stessa agli indirizzi mail indicati da genitori, alunni e dipendenti (si sottolinea anche qui l'importanza di utilizzare il campo ccn per l'invio, che a differenza del campo "a" e "cc" consente l'invio a più destinatari senza condividerne gli indirizzi);
- L'utilizzo delle modalità di comunicazione scuola famiglia messe a disposizione dal registro elettronico.

Gli interessati devono venire informati delle finalità didattiche su cui il trattamento si basa e sui possibili rischi associati. E' poi importante che ai docenti ed agli studenti vengano fornite le istruzioni e le conoscenze necessarie ad un utilizzo consapevole della strumentazione, ivi compresa la protezione dei dati personali propri e altrui.
L'informativa dovrà inoltre contenere un riferimento alla policy scolastica sull'utilizzo delle strumentazioni elettroniche, nella quale devono essere ben definite le responsabilità delle parti in causa. Nella policy dovrà essere chiaro che si potranno utilizzare, a scopi didattici, solamente quei servizi considerati "sicuri", per i quali il titolare provvederà a nominare i responsabili del trattamento.

Inoltre, sarà necessario rendere edotti gli interessati sui diritti di accesso, rettifica e cancellazione, ponendo preventivamente attenzione sui tempi necessari al trattamento dei dati. Particolare attenzione dovrà essere posta sul fatto che, una volta prodotti, i dati non potranno essere cancellati per un anno, in quanto atti amministrativi (o che verranno utilizzati a scopo di archivio, qualora la situazione lo preveda)

Ove applicabile: come si ottiene il consenso degli interessati?
La base legale del trattamento non è il consenso dell'interessato.

Come fanno gli interessati a esercitare i loro diritti di accesso e di portabilità dei dati?
La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati possono sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di rettifica e di cancellazione (diritto all'oblio)?
La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Come fanno gli interessati a esercitare i loro diritti di limitazione e di opposizione?
La scuola mette a disposizione degli interessati un modulo di esercizio dei propri diritti. Gli interessati posso sempre rivolgersi all'amministrazione tramite la modalità da loro preferita per l'esercizio degli stessi.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?
I servizi utilizzati devono essere selezionati anche sulla base della presenza di un contratto d'uso (fosse anche visualizzato e accettato in forma elettronica) che descriva l'ambito delle rispettive responsabilità e specifichi gli obblighi loro incombenti.
Nel caso in cui questo contratto non sia disponibile, il titolare provvederà a stipulare un contratto di nomina del responsabile.

In caso di trasferimento di dati al di fuori dell'Unione europea, i dati godono di una protezione equivalente?
I servizi previsti, e la G Suite in particolare, si basano sull'uso di server che possono anche essere localizzati nel territorio degli Stati Uniti d'America. Questo fatto ha delle criticità in relazione alla recente sentenza C.311/18 (Schrems II) con la quale la Corte di Giustizia ha dichiarato l'invalidità della decisione di adeguatezza Privacy Shield e che ha indotto Google stessa ad individuare nelle clausole contrattuali standard la base legale del trattamento. Cadendo quindi la valutazione di conformità a priori garantita dal privacy schield il Titolare è consapevole che spetta a lui verificare che le clausole contrattuali standard costituiscano una garanzia sufficiente per la tipologia di dati trattati. Dall'analisi condotta nella sezione successiva, riteniamo di poter affermare che il livello di protezione garantito è adeguato alla tipologia dei dati trattati limitata a quelli strettamente necessari al perseguimento delle finalità didattiche.

Si precisa che a seguito della sentenza Schrems II, intervenuta a luglio del 2020, l'Istituto scolastico ha valutato le possibili alternative all'uso della piattaforma G Suite adottata fin dal mese di marzo 2020 per garantire l'attuazione del dpcm dell'8 marzo 2020.

Una prima opzione considerata è stata quella di aderire alla licenza del software G suite enterprise, ovvero la versione a pagamento che consentirebbe di mantenere i dati trattati dalla piattaforma all'interno dei confini dell'Unione Europea. Questa soluzione si è rilevata troppo onerosa e non compatibile con le risorse a disposizione.

Una seconda opzione è stata la valutazione di servizi equivalenti forniti da altre aziende che utilizzassero server posti sul territorio europeo. La ricerca ha dato esito negativo.

E' stata infine valutata la possibilità di attrezzarsi in modo autonomo, con sistemi di file hosting in locale. Tale soluzione è risultata non percorribile per la mancanza di specifiche competenze all'interno dell'istituto.

Rischi

Misure esistenti o pianificate

Crittografia
I dati sono trattati tramite l'utilizzo di meccanismi di conservazione e comunicazione cifrati, ai fini di garantire la minimizzazione del rischio di acceso agli stessi.

Controllo degli accessi logici
L'accesso alle funzionalità delle piattaforme utilizzate deve essere regolato da un sistema di attivazione di account con permessi specifici, protetti da password, attivabili e disattivabili dall'amministratore del software (il D.S. o un suo delegato).

Archiviazione
Tutta la documentazione relativa all'attività Istituzionale dell'Amministrazione è regolata dalla normativa vigente in materia di archiviazione nella pubblica amministrazione, contenente indicazioni specifiche per la pubblica istruzione.

Minimizzazione dei dati
I dati vengono trattati e archiviati in forma minima, per quanto previsto dalla normativa vigente. I dati sensibili devono essere limitati a quelli strettamente necessari.

Lotta contro il malware
I sistemi scolastici sono protetti da malware con modalità di protezione sia hardware che software (firewall e antivirus). È inoltre opportuno fornire agli utilizzatori delle linee guida sull'utilizzo sicuro delle risorse elettroniche e digitali, che includano le istruzioni per una efficace lotta al malware.

Backup
I sistemi di didattica da remoto utilizzati per il trattamento devono essere provvisti di una modalità di backup.

Manutenzione
Viene effettuata regolarmente una attività di manutenzione nei confronti dei sistemi hardware scolastici. Il responsabile del trattamento garantisce inoltre il corretto funzionamento del software cloud di didattica da remoto.

Contratto con il responsabile del trattamento
I responsabili del trattamento devono essere nominati tali tramite la stipula di un contratto, ai sensi degli Artt. 28 e 29 del Reg. Ue 679/2016. La formalizzazione di esso può avvenire anche in forma elettronica con selezione di una opzione all'interno di un form.

Politica di tutela della privacy
L'amministrazione ha messo in atto una serie di misure orientate all'adeguamento della stessa alla normativa vigente. I dipendenti sono stati autorizzati al trattamento ai sensi dell'Art. 2-quaterdecies del D.Lgs. 196/2003, per l'esercizio delle loro funzioni.

Gestire gli incidenti di sicurezza e le violazioni dei dati personali
L'amministrazione ha emesso un regolamento interno per la gestione dei data breach, al cui interno sono specificate le modalità di gestione di tali fenomeni.

Formazione specifica del personale e degli interessati
Il personale e gli alunni saranno informati e istruiti riguardo alle modalità di utilizzo dei software, così da limitare il rischio di comportamenti che possano comportare un rischio per se e per gli altri.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Accesso a dati personali di minori con uso improprio degli stessi

Quali sono le principali minacce che potrebbero concretizzare il rischio?
Accesso ai dati da parte di amministrazioni extra unione europea.
Diffusione su piattaforme social dei dati personali acceduti, Scarsa sensibilità degli studenti alla privacy dei compagni. Queste ultime minacce sono da ricollegarsi a fenomeni di cyber bullismo, per l'analisi dei quali si rimanda alla più dettagliata DPIA sul cyberbullismo della scuola.
Quali sono le fonti di rischio?
Un dipendente che si renda responsabile di una negligenza a causa di un'insufficiente formazione e sensibilizzazione. Un utente (studente) che voglia utilizzare le informazioni per mettere in atto episodi di bullismo. Accesso di autorità governative statunitensi su server collocati su territorio extraeuropeo.
Quali misure fra quelle individuate contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate. In particolare, la proibizione dell'uso di dati personali non necessari all'attività formativa con particolare riferimento a quelli sensibili per i quali deve essere fatta una più rigorosa valutazione di stretta necessità.
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata. Le misure di sicurezza adottate e la limitazione dei dati personali a quelli necessari allo svolgimento dell'attività didattica riducono sensibilmente la gravità dei rischi. La natura dei dati personali trattati consente di valutare come limitata anche la gravità del rischio associato all'accesso ai medesimi da parte delle autorità governative statunitensi su server collocati al di fuori del territorio europeo. Questa eventualità è stata quella che ha fatto decadere la valutazione di idoneità a priori costituita dal privacy shield, idoneità che nel presente documento viene valutata dal titolare in relazione ai trattamenti effettivamente effettuati.
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Limitata, L'attivazione di sistemi di vigilanza interna e l'adozione e attuazione del regolamento, unito ad attività di sensibilizzazione possono essere in grado di limitare violazioni ad alto impatto. Trascurabile la probabilità di accesso alle informazioni detenute su server extraeuropei da parte di autorità governative statunitensi.

Modifiche indesiderate dei dati

Quali sarebbero i principali impatti sugli interessati se il rischio si dovesse concretizzare?
Potrebbe limitare le possibilità di intervento dell'amministrazione o dell'autorità giudiziaria.

Quali sono le principali minacce che potrebbero consentire la concretizzazione del rischio?
Accesso illecito ai dati e modifica degli stessi

Quali sono le fonti di rischio?
Errore umano, Fonti umane interne, che intervengano nella modifica dei dati

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate.
Come stimereste la gravità del rischio, in particolare alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Sebbene la violazione potrebbe portare ad una errata valutazione dell'alunno, le misure di backup e controllo degli accessi logici permetterebbero il recupero delle informazioni e la potenziale identificazione delle fonti di modifica.

Come stimereste la probabilità del rischio, specialmente con riguardo a minacce, fonti di rischio e misure pianificate?
Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda all'alienazione della disponibilità degli stessi agli studenti interessati, alla fine della fase di elaborazione concessagli.

Perdita di dati

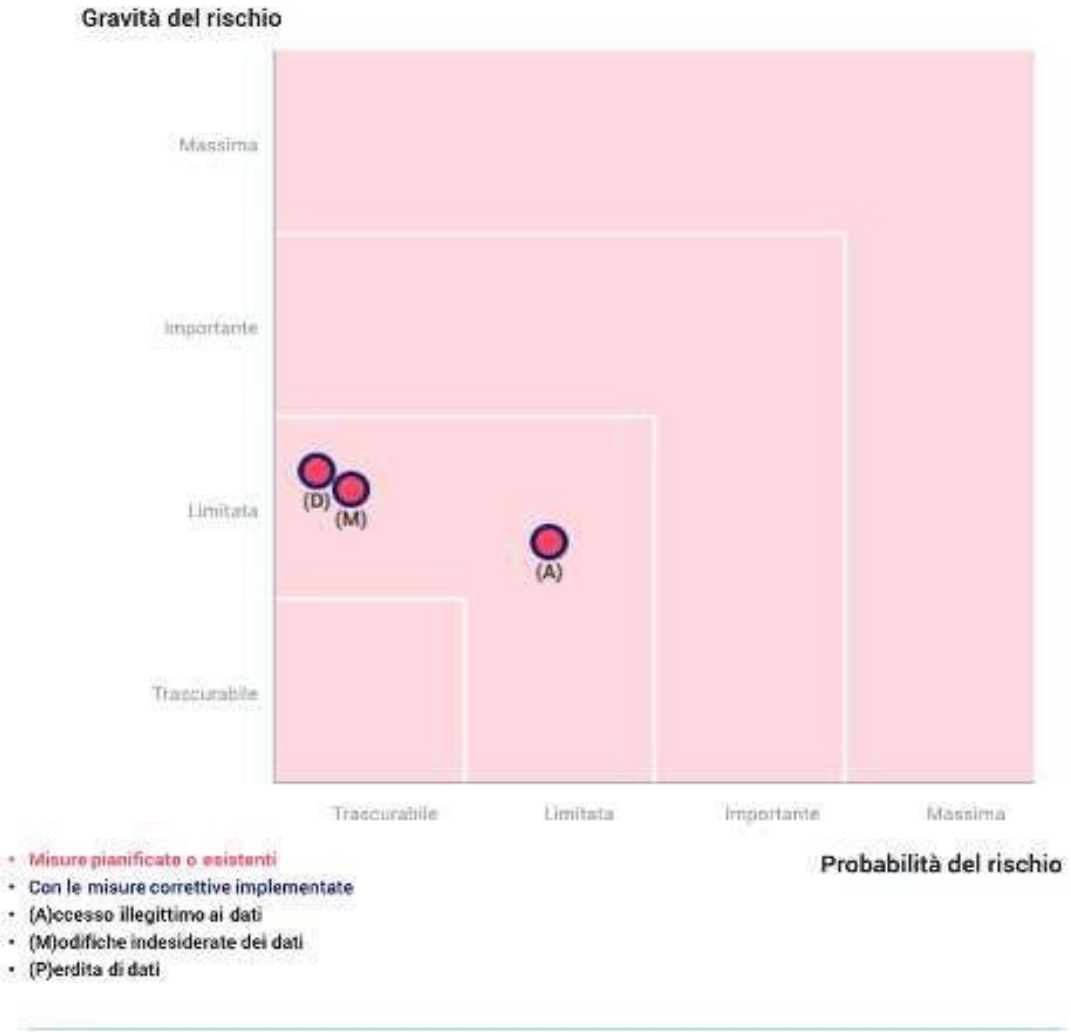
Quali potrebbero essere gli impatti principali sugli interessati se il rischio dovesse concretizzarsi?
Problematiche nella valutazione degli studenti da parte dei docenti e dell'amministrazione.
Quali sono le principali minacce che potrebbero consentire la materializzazione del rischio?
Distruzione dei server del servizio, Perdita dell'accesso ai documenti, errore umano

Quali sono le fonti di rischio?
Fonti umane interne, Fonti umane esterne (incaricati del responsabile del trattamento o dei sub-responsabili), Eventi naturali che possano influire sui dispositivi fisici di archiviazione.

Quali misure, fra quelle individuate, contribuiscono a mitigare il rischio?
Tutte le misure esistenti o pianificate individuate.
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?
Limitata, Possibile valutazione scolastica errata dell'alunno, a causa dell'incompletezza delle informazioni a disposizione del valutatore.
Come stimereste la probabilità del rischio, specialmente con riguardo alle minacce, alle fonti di rischio e alle misure pianificate?
Trascurabile, Appare impossibile che le fonti di rischio considerate concretizzino una minaccia basandosi sulle caratteristiche dei supporti, purché si proceda all'alienazione della disponibilità degli stessi agli studenti interessati.

ISTITUTO COMPRENSIVO “CASOPERO- FILOTTETE”
INDIRIZZO: VIA DELLA LIBERTA’ 60 – 88811 CIRO’MARINA (KR)
Cf: 91021410799 **Meccanografico**: KRIC82400D
Email: KRIC82400D @istruzione.it **Pec**: KRIC82400D@pec.istruzione.it

AGGIORNAMENTO DIPIA 13/01/2025



ISTITUTO COMPRENSIVO “CASOPERO- FILOTTETE”
INDIRIZZO: VIA DELLA LIBERTA’ 60 – 88811 CIRO’MARINA (KR)
Cf: 91021410799 **Meccanografico**: KRIC82400D
Email: KRIC82400D @istruzione.it **Pec**: KRIC82400D@pec.istruzione.it

AGGIORNAMENTO DIPIA 13/01/2025

