

	<p style="text-align: center;">ISTITUTO COMPRENSIVO STATALE "Santa Caterina" Cagliari</p> <p style="text-align: center;">Uffici di Direzione e Segreteria: Via Canelles, 1 - 09124 CAGLIARI Tel. 070662525 Fax 070652017 – C.M.: CAIC89300G Email PEC: caic89300g@pec.istruzione.it Email istituz.: caic89300g@istruzione.it Sito web: www.istitutocomprensivosantacaterina.edu.it</p>	
-----------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

Autore: D.S. Massimo Spiga
Validatore: Dr Mario Mureddu

Titolo: DPIA per l'adozione di strumenti supporti digitali per la formazione a distanza

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 delle stesse.

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 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 deve impegnare ad attribuire ai docenti il compito di supervisione sulle attività condotte con gli strumenti informatici 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 sulle piattaforme cloud, 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 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 fornitori 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 devono avvalersi 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.

Dati, processi e risorse di supporto

Quali sono i dati trattati?

La didattica da remoto permette di utilizzare le modalità di didattica cooperativa rese possibili dalle peculiari capacità di condivisione dati proprie delle strumentazioni digitali. Nel caso specifico, gli strumenti hardware di proprietà della scuola o degli studenti vengono utilizzati con l'intento di svolgere compiti didattici o di avere accesso a materiale formativo.

Le attività didattiche sono quindi svolte tramite una/più piattaforma/e elettronica/e 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.

Questo tipo di dati include dati relativi alla didattica degli alunni e dei docenti.

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, le convinzioni filosofiche o la condizione sanitaria degli interessati, che potrebbero essere di minore età.

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 delle fasi che presentano dei rischi potenziali. In particolare l'istituto attiva per gli studenti delle utenze personali sulla piattaforma cloud che dovranno essere utilizzate, con dispositivi di proprietà della scuola o degli studenti, per lo svolgimento delle attività istituzionali. 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 facenti utilizzo di tecnologie *cloud*, che permettono la condivisione e organizzazione dei compiti assegnati. Tali tecnologie possono, talvolta, basarsi su server extra-ue, e in tal caso è necessario 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 suscettibili di diventare atti amministrativi scolastici.

Quali sono le basi legali che rendono lecito il trattamento?

La base legale del trattamento è l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento; In particolare il trattamento viene effettuato sulla base del Piano Triennale dell'Offerta Formativa dell'Istituto che prevede l'utilizzo di sistemi digitali di supporto alla didattica per il conseguimento delle proprie finalità istituzionali.

L'utilizzo degli strumenti di formazione a distanza ha fondamento anche nei seguenti riferimenti normativi:

- D. Lgs 82/2005 (Codice che traccia il quadro legislativo entro cui deve attuarsi la digitalizzazione della pubblica amministrazione)
- D. L. 179/2012 convertito con L. 221/2012 (che ha introdotto per le istituzioni scolastiche l'uso del registro elettronico)
- D. Lgs 297/1994 (Approvazione del testo unico delle disposizioni legislative vigenti in materia di istruzione, relative alle scuole di ogni ordine e grado) che all'art. 1 stabilisce la libertà di insegnamento.

Si rileva che, se pure è caduto lo stato di emergenza dovuto alla diffusione di Covid 19, le istituzioni scolastiche sono invitate ad adottare strumenti che consentano lo svolgimento della Didattica Digitale Integrata che prevede un uso più maturo e proficuo degli strumenti informatici e telematici intesi come strumenti complementari alla didattica in presenza e che, in caso di emergenza, possano garantire lo svolgimento dell'attività didattica a distanza.

Nel caso in cui gli elaborati degli studenti inseriti nelle piattaforme utilizzate vengano considerati validi ai fini della valutazione (i c.d. compiti di valutazione), 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.

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 informazioni necessaria al corretto svolgimento delle loro funzioni. I principi di adeguatezza, pertinenza e minimizzazione dovranno essere applicati in modo particolarmente rigoroso per i dati particolari di cui all'art. 9 del GDPR (dati sensibili) che dovranno essere trattati solo se strettamente necessari.

I medesimi principi dovranno anche essere presi in considerazione nel valutare i dati ed i documenti che gli alunni, ma anche i docenti, potranno in modo autonomo caricare sulla piattaforma in cloud. E' peraltro importante vigilare affinché i dati trattati non esulino dalle esigenze formative connesse all'ambito didattico o, più genericamente, istituzionale.

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, essa non può essere modificata o cancellata 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.

In riferimento al periodo di conservazione dei documenti di distinguono 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 2016/679. 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 devono venire specificati i possibili rischi associati. Durante il processo didattico stesso verranno forniti agli studenti le conoscenze necessarie ad un utilizzo consapevole della strumentazione, ivi compresa la protezione dei dati personali propri e altrui.

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?

Il consenso non costituisce base legale del trattamento e non viene richiesto agli interessati.

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 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 limitazione e di opposizione?

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.

Gli obblighi dei responsabili del trattamento sono definiti con chiarezza e disciplinati da un contratto?

I servizi utilizzati sono stati 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 specifica gli obblighi loro incombenti.

Nel caso in cui il contratto non lo preveda esplicitamente, il titolare provvederà a formalizzare con apposito documento la nomina a responsabile del trattamento.

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

L'elenco dei servizi ammessi prevede solamente e ove fosse necessario l'utilizzo di server posti nello spazio dell'Unione Europea. Qualora fosse necessario utilizzare servizi che trasferiscano dati all'esterno di quest'area, potranno essere ammessi solamente servizi che trasferiscano i dati negli Stati Uniti d'America o nella Svizzera, che garantiscano misure di sicurezza comparabili con quelli previsti dalla normativa di riferimento regolati da Clausole Contrattuali Standard (art. 46 GDPR), e previa analisi sostanziata in una valutazione di impatto del trasferimento (TIA Transfer Impact Assessment).

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 accesso 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 sono 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

Deve essere 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 (anche con accettazione di condizioni mediante flag su modulo elettronico)

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 nominati incaricati 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.

Accesso illegittimo ai dati

Quali potrebbero essere i principali impatti sugli interessati se il rischio si dovesse concretizzare?

Violazione di riservatezza di dati personali anche di natura sensibile (ove ne venga ritenuto necessario il trattamento) con possibili atti di cyberbullismo

Quali sono le principali minacce che potrebbero concretizzare il rischio?

Pubblicazione su piattaforme social di dati personali, Scarsa sensibilità degli studenti alla privacy propria e dei compagni, Episodi di Cyberbullismo, Negazione del diritto all'oblio

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 e di minore età) che voglia utilizzare le informazioni per mettere in atto episodi di bullismo

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?

Massima. L'utilizzo improprio delle piattaforme didattiche, e specialmente la pubblicazione di informazioni sensibili di minori a scopo di Cyberbullismo potrebbe avere importanti conseguenze negative sulla vita delle vittime, specie in un periodo delicato quale è l'adolescenza. Ciò potrebbe causare disturbi psicologici a lungo termine o permanenti.

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, con i principi di minimizzazione in esso stabiliti, unito ad attività di sensibilizzazione possono essere in grado di limitare violazioni ad alto impatto. Tuttavia, vista anche l'elevata imprevedibilità dei comportamenti dei minori in questione, non possono essere esclusi comportamenti inappropriati che possano portare a conseguenze anche gravi per gli interessati.

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 ove si considerino le misure di sicurezza adottate. Si consideri anche che i fornitori delle piattaforme cloud devono garantire l'integrità dei dati trattati anche per mezzo di idonei sistemi di backup che consentirebbero il ripristino dei dati modificati.

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.

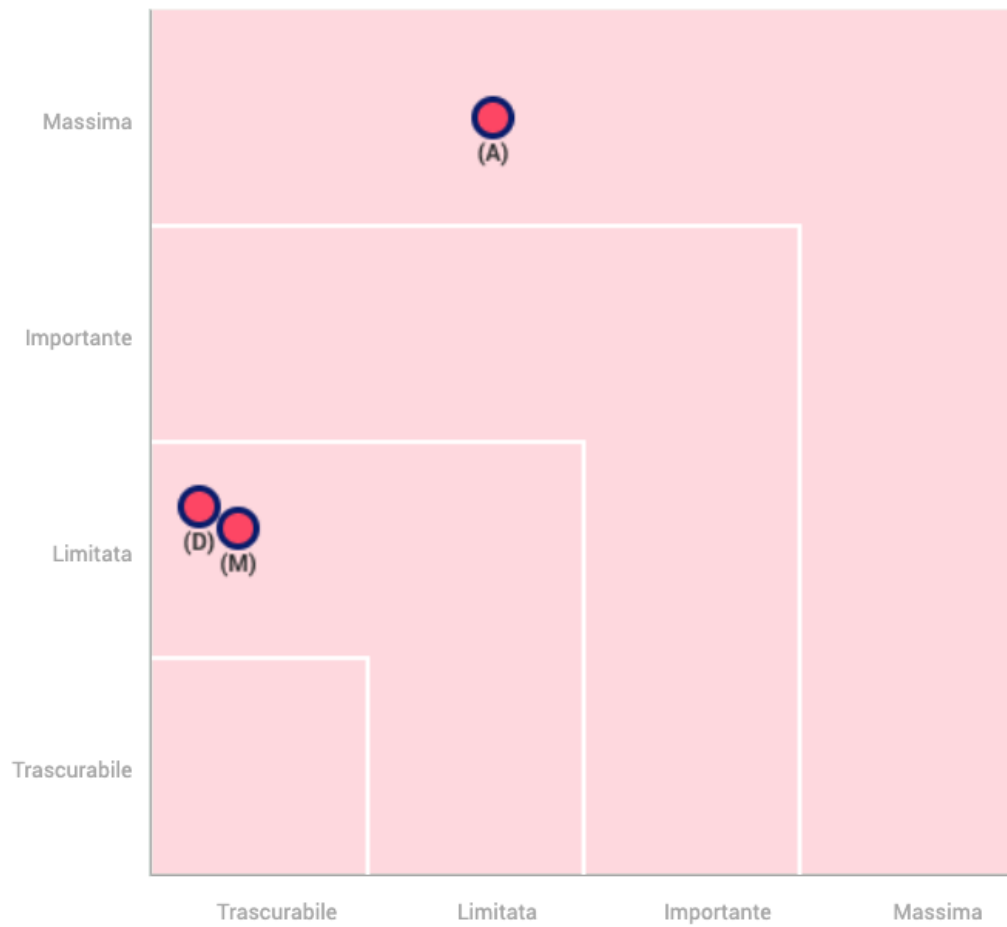
Come stimereste la gravità del rischio, specialmente alla luce degli impatti potenziali e delle misure pianificate?

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 ove si considerino le misure di sicurezza adottate. Si consideri anche che i fornitori delle piattaforme cloud devono garantire l'integrità dei dati trattati anche per mezzo di idonei sistemi di backup.

Gravità del rischio



- **Misure pianificate o esistenti**
- **Con le misure correttive implementate**
- (A)ccesso illegittimo ai dati
- (M)odifiche indesiderate dei dati
- (P)erdita di dati

Probabilità del rischio

Impatti potenziali

Diffusione di dati personal.
Diffusione di dati concerne
Cyberbullismo
Modifica della documentaz
Valutazione impropria degli
Problematiche nella valutaz

Minaccia

Pubblicazione su piattaform
Scarsa sensibilità degli st...
Episodi di cyberbullismo
Negazione del diritto all'o..
Non opportuna gestione deg
Errori umani

Fonti

Un dipendente che si renda
Un utente (studente e di mi
Modifica a posteriori della.
Docenti
Studenti

Misure

Prevenzione delle fonti di .
Minimizzazione dei dati
Controllo degli accessi log.
Archiviazione

Accesso illegittimo ai dati

Gravità : Massima

Probabilità : Limitata

Modifiche indesiderate dei dati

Gravità : Limitata

Probabilità : Trascurabile

Perdita di dati

Gravità : Limitata

Probabilità : Trascurabile

Conclusioni

Gli organi collegiali del nostro istituto hanno deliberato in merito all'utilizzo delle moderne tecnologie informatiche e telematiche nello svolgimento delle attività istituzionali di competenza delle scuole con l'obiettivo specifico di migliorare la qualità dell'attività didattica e formativa. Tali tecnologie sono peraltro di uso comune tra i nostri studenti per cui è importante che l'utilizzo in ambito scolastico serva a promuoverne un uso più efficace e consapevole anche in relazione ai rischi associati ai trattamenti di dati personali operati.

L'adozione degli strumenti è stata operata in piena emergenza pandemica causata da Covid 19 seguendo le indicazioni del Ministero dell'Istruzione che, per favorire scelte tempestive ed efficaci, aveva pubblicato un elenco di risorse gratuite a disposizione delle scuole.

Nell'operare la scelta fra queste risorse sono stati presi in considerazione i seguenti elementi:

- Sicurezza
- Affidabilità
- Diffusione
- Semplicità d'uso e di gestione
- Costo
- Presenza di certificazione AGID

Al termine di tale valutazione comparativa la scelta è caduta sulla piattaforma messe a disposizione da Google a causa delle garanzie fornite in termini di affidabilità, sicurezza, diffusione, facilità di gestione e di utilizzo e per il fatto che la soluzione era proposta gratuitamente agli istituti scolastici. Si rileva che la scelta della soluzione è antecedente la sentenza Schrems II e che, a seguito di questa, il fornitore ha prontamente provveduto a individuare nelle Clausole Contrattuali Standard lo strumento per assicurare la conformità dei trattamenti al GDPR. In seguito alla sentenza Schrems II si è tuttavia proceduto a fare una prima DPIA sull'uso delle piattaforme cloud in ambito didattico di cui il presente documento costituisce l'ultimo aggiornamento.

A seguito dell'analisi condotta abbiamo stimato l'entità dei rischi associati ai trattamenti operati sulla piattaforma adottata e le misure atte a contenere questi rischi al di sotto di un livello accettabile. A questo proposito è opportuno chiarire che l'uso di qualunque strumento informatico comporta dei rischi per i dati personali trattati e che la valutazione che deve essere fatta non è quella di conseguire il rischio zero (possibile solo se si rinuncia a qualunque strumento) ma quello di contenere i rischi al di sotto di una soglia accettabile. L'assenza di oggettivi impedimenti all'uso della piattaforma adottata è peraltro dimostrata dal fatto che questa è un servizio cloud per la PA certificato AGID e che, al momento dell'adozione, era presente nell'elenco delle risorse consigliate dal Ministero dell'Istruzione.

Valutata la conformità alle disposizioni del GDPR della piattaforma già adottata si precisa che non si ritiene di poter condurre alcuna valutazione comparativa ai sensi dell'art. 68 del d. lgs. 7/3/2005 n. 82 considerata l'assenza di qualunque soluzione con software libero o a codice aperto che possa essere utilizzabile nel nostro contesto. Soluzioni quali, ad esempio, BigBlueButton, Moodle, EduMEET, Jitsi, NextCloud non possono essere da noi prese in considerazione per la difficoltà di installazione e di gestione dei sistemi in relazione al personale scolastico che sarebbe chiamato a svolgere tali attività. Si evidenzia peraltro che la mancanza di adeguate competenze tecniche da parte del personale scolastico su tali piattaforme open source esporrebbe i dati personali trattati a rischi ben più rilevanti rispetto a quelli valutati in questa DPIA per l'uso di soluzioni cloud commerciali.